RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 276 639**
(A n'utiliser que pour les commandes de reproduction).

A1

# DEMANDE DE BREVET D'INVENTION

(21) N° **75 16531**

(54) **Système de traitement de transactions entre un ordinateur hôte et des terminaux éloignés.**

(51) Classification internationale (Int. Cl.²). G 06 F 13/00.

(22) Date de dépôt ..... 21 mai 1975, à 10 h.

(33) (32) (31) Priorité revendiquée : *Demande de brevet déposée aux Etats-Unis d'Amérique le 25 juin 1974, n. 483.084 aux noms des inventeurs.*

(41) Date de la mise à la disposition du public de la demande ..... B.O.P.I. — «Listes» n. 4 du 23-1-1976.

(71) Déposant : Société dite : INTERNATIONAL BUSINESS MACHINES CORPORATION, résidant aux Etats-Unis d'Amérique.

(72) Invention de : Thomas G. Anderson, William A. Boothroyd et Richard C. Frey.

(73) Titulaire : *Idem* (71)

(74) Mandataire : Gérard Bonneau, Département de Propriété Industrielle IBM.

La présente invention concerne un système de traitement de transactions comprenant un ordinateur hôte comportant un fichier de base central, en communication avec des terminaux éloignés qui permettent l'exécution de transactions telles que la délivrance d'espèces ou le transfert de fonds de compte à compte.

Pour répondre aux besoins du public et pour des raisons économiques, de nombreux systèmes différents ont été réalisés pour exécuter des transactions demandées par un utilisateur. Un exemple d'un de ces systèmes est une machine à payer les chèques. Une telle machine lit les données d'un chèque inséré dans la machine et délivre un montant en espèces égal au montant du chèque si le chèque a été reconnu conforme. D'autres systèmes ont été réalisés qui sont destinés à être utilisés avec des cartes de crédit.

Un système connu de cartes de crédit garde en mémoire des informations de comptes de cartes de crédit dans un fichier de base central.En réponse à un numéro de compte provenant d'un terminal éloigné, le système fournit des informations relatives au compte. Par exemple, le système peut indiquer que la durée de validité de la carte a expiré, que la carte a été volée ou il peut indiquer le montant en francs du crédit disponible. Après qu'une transaction a été achevée, le système ajuste les informations en mémoire pour entrer la transaction en compte.

D'autres systèmes de cartes de crédit qui sont fréquemment utilisés par les banques pour améliorer leurs services pendant les périodes de surcharge de travail ou pour poursuivre leurs services pendant les heures de fermeture permet la délivrance d'espèces ou la réception de dépôts, au moyen d'un terminal. Un tel terminal comporte typiquement un mécanisme pour recevoir et lire les informations portées sur une carte de crédit, un clavier, un dispositif d'affichage et des ouvertures d'entrée et de sortie de documents. Le terminal peut fonctionner en combinaison avec un fichier central ou comme unité indépendante. Une sécurité accrue pour la délivrance d'espèces est obtenue en délivrant un numéro d'identification personnel avec chaque carte de crédit. Une transaction effectuée au moyen d'une carte de crédit n'est alors autorisée que lorsqu'un numéro d'identification correspondant au numéro de compte lu sur la carte de crédit est entré au moyen du clavier. Cette correspondance requise empêche qu'une personne ayant volé ou trouvé une carte de crédit puisse recevoir des espèces d'un terminal. Si un terminal fonctionne en combinaison avec un fichier de base central, la correspondance entre les numéros de compte et les numéros d'identification peut être choisie au hasard mais, fréquemment, le numéro d'identification peut être calculé à partir du numéro de compte conformément à un code prédéterminé. Cette relation prédéterminée permet à un terminal indépendant de contrôler

le numéro d'identification en comparant le numéro d'identification au numéro de compte suivant un algorithme approprié.

Bien que cette technique de double identification par la carte de crédit et le numéro d'identification améliore la sécurité des terminaux de délivrance d'espèces, elle présente encore des faiblesses qui peuvent être exploitées pour avoir accès aux montants importants en espèces qui sont conservés dans les terminaux. Par exemple, il peut être nécessaire d'employer un grand nombre d'opérateurs, de programmeurs d'analyses et autres employés à l'endroit où est conservé le fichier central qui ont, de ce fait, accès aux informations mises en mémoire dans le fichier central de l'ordinateur hôte. Il serait possible à ces personnes de rassembler des listes du numéros de compte et des numéros d'identification correspondants pour les utiliser avec des cartes de crédits contrefaites ou volées afin d'obtenir des espèces.

Un problème grave concerne la sécurité de l'algorithme de chiffrement dans le cas des terminaux qui sont capables d'un fonctionnement indépendant. De nombreux opérateurs et personnes du service d'entretien doivent être employés pour assurer le fonctionnement journalier des terminaux de délivrance d'espèces. Par exemple, une ou deux personnes à chaque succursale de banque peut avoir accès à l'intérieur des terminaux de délivrance d'espèces. Fréquemment, ces personnes peuvent avoir accès à la clé de chiffrement pour l'entretien normal. Alternativement, avec seulement une formation pratique peu importante, ces personnes pourraient apprendre à obtenir la clé en mesurant les signaux électriques sur les circuits internes. Une fois que la clé de chiffrement est connue, une correspondance entre un grand nombre de numéros de comptes et de numéros d'identification peut être établie.

Un autre problème de sécurité qui peut se poser résulte de la transmission des informations de compte et des informations d'identification entre un terminal et un fichier central d'un ordinateur. Ces transmissions sont fréquemment effectuées en utilisant les lignes de communications publiques et sont, par conséquent, susceptibles d'être surveillées par un grand nombre de personnes. Le chiffrement est fréquemment utilisé pour améliorer la sécurité des communications mais toute personne capable de déchiffrer le code ou d'avoir accès au code a alors la possibilité d'extraire et d'établir une liste de correspondances entre des informations de cartes de crédit et des numéros d'identification en surveillant ces transmissions. En outre, en engendrant un échange fictif de communication une personne pourrait avoir accès au fichier central et transférer de manière frauduleuse des fonds entre les comptes du fichier central. Ainsi, bien qu'ils soient protégés des voleurs ordinaires, les systèmes classiques qui utilisent cette technique

de double identification ne sont pas convenablement protégés contre un voleur plus subtil ayant une connaissance des installations de traitement des données modernes.

L'objet de la présente invention est donc un système de traitement de transactions comportant un ordinateur hôte ayant un fichier central constitué par des infomations mises en mémoire relatives à un grand nombre de comptes et une série de terminaux. L'ordinateur hôte fonctionne de façon à approuver ou à refuserdes transactions indiquées, à modifier les informations de comptes en mémoire pour entrer en compte, de façon appropriée, les transactions exécutées et à fournir des informations d'assitance aux terminaux. Les terminaux de transaction sont des unités fonctionnellement indépendantes qui sont connectées de façon à pouvoir communiquer avec l'ordinateur hôte à partir de lieux disséminés. Chaque terminal comporte un sous-système de manipulation de documents pour les espèces ou les états de transaction, un sous-système de lecture de cartes de crédit, un sous-système de communication avec l'ordinateur hôte, un sous-système de communication avec l'utilisateur et un sous-système de commande des opérations qui comporte un microprocesseur programmable.

Le sous-système de manipulation des documents comporte un mécanisme de réserve d'espèces, un mécanisme d'entraînement pour délivrer des espèces à un utilisateur sous la supervision et la commande du microprocesseur et un distributeur d'états de transaction qui délivre des états imprimés sous la commande du micro-processeur. Le sous-système de lecture des cartes de crédit fonctionne sous la commande du microprocesseur pour recevoir et lire les cartes de crédit d'utilisateurs qui peuvent être soit rendues à l'utilisateur soit retenues après le traitement d'une demande de transaction. Le sous-système de communication avec l'ordinateur constitue une interface servant à assurer la transmission convenable des informations entre un terminal et l'ordinateur conformément à des formats de communication prédéterminés. Le sous-système de communication avec l'utilisateur fonctionne en réponse au microprocesseur pour commander l'accès de l'utilisateur au terminal et comporte un clavier recevant les ordres de l'utilisateur et un dispositif d'affichage servant à guider l'utilisateur par une action conjuguée avec celle du clavier.

Un utilisateur qui désire effectuer une transaction doit insérer une carte de crédit dans un terminal puis entrer les informations d'identification personnelle et de demande de transaction au moyen du clavier. Le terminal code alors facultativement une partie prédéterminée des informations de la carte de crédit en utilisant une première clé de chiffrement pour obtenir des informations d'identification chiffrées qui peuvent être l'objet

d'une vérification afin de déterminer si elles correspondent à une partie prédéterminée des informations d'identification entrées sur le clavier. En l'absence d'une correspondance prédéterminée, la transaction est terminée, l'ordinateur est informé par un message et la réponse de l'ordinateur définit l'action qui doit être prise vis à vis de la carte, qui est sélectivement rendue à l'utilisateur ou retenue. Si une correspondance est déterminée, les informations d'identification entrées sont codées en utilisant une seconde clé de chiffrement qui peut être la même que la première clé de chiffrement. Les informations d'identification chiffrées sont alors combinées à des informations variables, telles qu'un numéro de transaction séquentiel ou un compte d'espèces, pour empêcher la transmission répétitive de zones chiffrées d'une manière identique puis elles sont à nouveau codées en utilisant une troisième clé, ou clé de transmission. Ce procédé de chiffrement permet au fichier central de l'ordinateur de conserver en mémoire non le numéro d'identification mais seulement un numéro d'identification chiffré. Le fichier central a ainsi sa sécurité assurée vis à vis d'une extraction clandestine d'une liste de correspondance de numéros de compte et de numéros d'identification à partir de laquelle des cartes contrefaites pourraient être crées. Les informations d'identification chiffrées sont combinées avec les informations de la demande de transaction et les informations de la carte de crédit en clair et sont alors communiquées à l'ordinateur . Une séquence d'exécution de transaction en trois parties commence par un message de demande de transaction qui transmet à l'ordinateur le numéro d'identification chiffré qui a été combiné à des données variables puis rechiffré, les informations de la carte de crédit et les informations de demande de transaction entrées au moyen du clavier. Par exemple, l'utilisateur peut demander la délivrance de 500 F sur son compte de carte de crédit. A la réception d'une demande, l'ordinateur contrôle la correspondance entre le numéro d'identification codé transmis et le numéro d'identification codé mis en mémoire dans son fichier central, contrôle les restrictions apportées à l'utilisation du compte, telles qu'une limite maximale de crédit et, si tout est en ordre, il transmet un message de réponse autorisant la transaction. Si un point quelconque n'est pas en ordre, l'ordinateur hôte refuse la transaction.

De même que le message de demande de transaction, le message de réponse qui suit comporte une partie chiffrée contenant une commande d'action et des données variables, telles qu'un nombre indiqué par un compteur d'espèces ou un numéro de transaction. Après que les informations codées ont été combinées à des informations en clair, telles que des informations d'état de transaction et des informations d'affichage, le message de réponse est transmis au terminal demandeur. A la réception par le terminal de transactions

demandeur du message de réponse de transaction, le terminal effectue le déchiffrement, vérifie la correction des données variables pour se garantir vis à vis des risques d'erreur puis exécute les actions commandées. Le terminal engendre alors un message d'état pour informer l'ordinateur de l'exécution ou de l'annulation de la transaction ou de toute condition d'erreur au terminal. Une partie chiffrée du message d'état comporte le numéro de transaction, le nombre d'octets d'état du message et l'état du compteur d'espèces.

L'ordinateur agit en réponse en comptabilisant de la façon appropriée la transaction indiquée, cette opération étant effectuée soit en enregistrant la transaction soit en mettant à jour le fichier central. Si une condition d'erreur est indiquée, l'ordinateur peut transmettre un message de commande pour essayer de corriger l'erreur ou fermer le terminal si l'erreur ne peut pas être corrigée. L'utilisation de cette technique de message de données rend très difficile le déchiffrement des clés de chiffrement et assure une redondance des communications pour garantir que l'ordinateur et un terminal répondent aux messages corrects. En outre, la correspondance entre les numéros d'identification personnels et les numéros de compte est protégée par un système de chiffrement qui évite la nécessité de mettre en mémoire ces deux numéros dans le fichier central.

D'autres objets, caractéristiques et avantages de la présente invention ressortiront mieux de l'exposé qui suit fait en référence aux dessins annexés à ce texte, qui représentent un mode de réalisation préféré de celle-ci.

La figure 1 est un schéma bloc fonctionnel représentant un système d'exécution des transactions conformément à l'invention;

la figure 2 est un schéma-bloc fonctionnel représentant un terminal de transactions utilisé dans le système d'exécution de transactions représenté sur la figure 1.;

la figure 3 est un organigramme représentant la manière suivant laquelle une demande de transaction entreprise par un utilisateur est initialement traitée par un terminal de transactions;

la figure 4 est un organigramme représentant la manière suivant laquelle les demandes de transaction reçues sur un terminal de transaction sont traitées par un ordinateur hôte;

TABLE DES MATIERES



INTRODUCTION

Un système d'exécution de transactions 10 conformément à l'invention comporte un ordinateur hôte 12 et un certain nombre de terminaux de transactions d'utilisateurs 14 en communication avec l'ordinateur. L'ordinateur 12 comporte une unité de traitement centrale 16, telle qu'un ordinateur IBM 370, une unité de commande de transmission 18, telle que l'unité de commande IBM 3705, et un fichier central 20 qui peut comporter une mémoire à accès sélectif modifiable, des unités à bande magnétique et des disques magnétiques. L'unité de traitement centrale effectue les opérations arithmétiques et logiques qui sont nécessaires pour commander le fonctionnement de l'ordinateur 12 et pour traiter les informations qui sont reçues par l'intermédiaire de l'unité de commande de transmission 18 ou mises en mémoire dans le fichier central 20. Le fichier central 20 conserve en mémoire les informations relatives à chaque élément de l'ordinateur 12. Par exemple, lorsque le client est une banque, le fichier central peut conserver en mémoire des informations de comptes concernant les comptes à cartes de crédit, les comptes d'épargne, les comptes courants et autres comptes de la banque ainsi que les informations d'états de salaires et des informations relatives à l'état financier des opérations de la banque.

Chaque compte peut être typiquement adressé au moyen d'un numéro de compte et peut comporter des informations courantes sur ce compte, telles que la situation actuelle du compte, une liste de transactions du compte pendant une période de temps prédéterminée, les numéros d'identification personnels codés pour les personnes qui sont autorisées à utiliser le compte, une limite maximale de crédit et toutes les autres informations que

la banque peut désirer mettre en mémoire en tant que partie d'un compte. L'unité de commande de transmission 18 sert d'interface entre l'unité de traitement 16 et une série de canaux de communication 22. L'unité de commande 18 organise les informations reçues par l'unité de traitement centrale 16 suivant une discipline de communications et maintient la synchronisation des communications.

Un terminal transactions peut être connecté pour communiquer avec l'ordinateur 12 de diverses manières qui sont en nombre presqu'illimité, les divers procédés représentés sur la figure 1 n'étant donnés qu'à titre d'exemple. Par exemple, un terminal peut être connecté directement à l'unité de commande de transmission 18 soit par une voie de communication locale, telle qu'un câble 24, pour un terminal de transaction d'utilisateur local 26, soit par une voie de communication publique ou radio 28, pour un terminal de transactions d'utilisateurs éloigné 30. Alternativement un terminal peut être connecté à l'ordinateur 12 par l'intermédiaire d'une unité de commande 32, telle que l'unité IBM 3601 en étant, dans ce cas, soit directement connectée à l'unité de commande 32, par exemple par un câble, comme le terminal 36, soit connectée dans une boucle de communications 38. Bien que d'autres dispositifs puissent être inclus dans la boucle, la boucle de communication a été représentée à titre d'exemple comme comportant un premier poste de travail de caissier 40, un second poste de travail de caissier 42, un premier terminal de transactions d'utilisateurs 44 et un second terminal de transactions 46. Bien que la boucle de communications 38 puisse comporter des voies de communication à distance, telles que des voies de communication radio ou des communications sur les lignes téléphoniques dans le cas d'un système bancaire, l'unité de commande 32 peut être située dans une succursale de la banque tandis que tous les terminaux de traitement des données situées dans la succursale sont connectés dans la bouce 38. L'unité de commande 32 peut, elle-même, être connectée à un canal de communication 22 de l'unité de commande de transmission 18 soit directement soit par l'intermédiaire d'une voie de communication 48, telle qu'une ligne téléphonique comme représenté sur la figure 1, ou elle peut être elle-même connectée dans une boucle de communication, telle que la boucle 38 raccordée à un canal de communication 22 de l'unité de commande de transmission 18.

En général, l'unité de commande 32 sert uniquement de dispositif de relais pour les informations qui sont transmises autour de la boucle mais elle peut également servir de processeur hôte. Lorsqu'elle sert de processeur hôte, l'unité de commande 32 doit mettre en mémoire les informations d'exécution des transactions en vue de leur traitement ultérieur par l'ordinateur

12 et doit fournir les fonctions d'assistance remplies par le processeur hôte qui sont nécessaires pour le fonctionnement d'un terminal 14.

I - Terminal d'exécution de transactions

Bien que la manière particulière suivant laquelle le terminal de transactions est réalisé ne soit pas critique pour la mise en oeuvre de la présente invention, un mode de réalisation préférentiel du terminal de transactions 14 a été représenté sur la figure 2. Le terminal 14 est, dans son ensemble, de nature modulaire et comporte un microprocesseur programmable 72 couplé à un certain nombre de sous-systèmes du terminal par un bus d'informations 52. Le fonctionnement du micro-processeur 72 est commandé par des signaux d'horloge fournis par un générateur de signaux d'horloge 68 et le microprocesseur est connecté à un module de mémoire de données 74 qui comporte à la fois une mémoire à accès sélectif susceptible modifiable (RAM) et une mémoire morte (ROS). La partie de mémoire morte de la mémoire de données 74 conserve en mémoire les divers programmes servant au fonctionnement du microprocesseur 72. La partie de mémoire à accès sélectif de mémoire de données 74 sert de mémoire "bloc-note" pour l'exécution du programme.

II - Bus d'informations du terminal

Le microprocesseur 72 ne communique avec les sous-systèmes modulaires que par l'intermédiaire du bus d'informations du terminal 52. Cette technique d'interconnexion des sous-systèmes modulaires avec le microprocesseur 72 par l'intermédiaire du bus 52 permet au microprocesseur 72 de recevoir des informations détaillées sur l'état du terminal et d'assurer une direction détaillée des opérations du terminal sans qu'il soit nécessaire d'utiliser un grand nombre de connexions d'entrée et de sortie d'informations. La tâche de détecter les informations d'état du terminal est effectuée par les sous-systèmes individuels du terminal. Ces informations sont alors transférées au microprocesseur 72 sur sa commande. D'une manière similaire, les circuits de commande servant à exécuter les commandes du microprocesseur sont contenus dans les modules des sous-systèmes. Les commandes du microprocesseur sont des commandes de base. Chaque commande réalise une opération élémentaire du sous-système telle que la mise sous tension et la mise hors tension d'un moteur, l'affichage ou l'impression d'un caractère, l'entraînement d'un billet ou la lecture d'un caractère de communication. Le bus 52 comporte une ligne de signaux de restauration du système, 9 lignes de signaux de données en entrée (8 bits plus le bit de parité) pour transmettre des informations provenant du processeur 72 à un sous-système connecté et des lignes de signaux de commande pour commander le transfert d'informations au bus et le transfert d'informations à partir du bus 52.

III - Sous-système d'assistance du processeur

L'un des sous-systèmes opérationnels qui est connecté par l'intermédiaire du bus 52 au microprocesseur 72 est le sous-sytème d'assistance du microprocesseur 60. Le sous-système 60 fournit un support matériel au microprocesseur 72 à l'inverse des autres sous-systèmes du terminal qui remplissent des fonctions relatives à des aspects particuliers du fonctionnement du terminal 14.

Le sous-système 60 reçoit un signal d'horloge à une fréquence de 1 MHz du générateur de signaux d'horloge 68 et divise ce signal pour engendrer des signaux d'horloge de plus basse fréquence qui sont utilisés dans les autres sous-systèmes. Un signal d'horloge de plus basse fréquence est utilisé pour la génération de commandes d'interruption périodiques à des intervalles de 10 millisecondes. Ces commandes d'interruption provoquent la génération, par le circuit logique d'interruption que comporte le sous-système 60, d'une interruption du microprocesseur toutes les 10 millisecondes. Le microprocesseur 72 utilise ces interruptions périodiques commandées par l'horloge pour entretenir une base de temps de commande d'évènements pour les diverses opérations du terminal 14. Le circuit logique de restauration prévu dans le sous-système 60 commande la ligne de restauration du bus 52. L'activation de cette ligne de restauration provoque l'initialisation du processeur 72 ainsi que de tous les modules qui sont connectés au bus 52 et annule toute transaction d'utilisateur en instance. Le processeur est ramené à une instruction de programme prédéterminée à partir de laquelle l'exécution du programme peut recommencer à la suite de la restauration. Le signal de restauration est engendré en réponse au branchement de l'alimentation, à l'actionnement d'un interrupteur de restauration ou à un signal d'immobilisation provenant d'un détecteur d'immobilisation prévu dans le sous-système 60. Le détecteur d'immobilisation surveille les lignes de commande du bus 52 et engendre un signal d'immobilisation lorsque l'activité du bus cesse pendant une période de temps qui est suffisante pour indiquer que le microprocesseur 72 ne fonctionne pas convenablement. Un détecteur de fonctionnement répond aux signaux de demande d'interruption de l'horloge et engendre un signal de fonctionnement qui est maintenu actif tant que le microprocesseur répond régulièrement aux demandes. Si une période de temps prédéterminée s'écoule sans le traitement d'une demande d'interruption de l'horloge, le détecteur de fonctionnement termine le signal de fonctionnement. Le sous-système 60 comporte également un circuit logique de traitement des données de lecture qui reçoit les chaines d'informations séquentielles lues sur une carte de crédit d'utilisateur, sépare les données des informations de synchronisation, convertit les données de série en parallèle et place les données sur le bus 52 en vue de leur traitement par le microprocesseur 72.

IV - Sous-système de commandes des fonctions mécaniques

Un sous-système de commande des fonctions mécaniques 61 assure les manipulations mécaniques effectives des divers dispositifs matériels du terminal 14. Le sous-système 61 qui, de même que les autres sous-systèmes, n'a aucune capacité de branchement ou d e prise de décision exécute des commandes de base élémentaires fournies par le microprocesseur 72 et recueille les informations sur l'état physique des divers dispositifs fonctionnels matériels en vue de leur communication au multiprocesseur 72. Pour donner un exemple de la nature élémentaire individuelles des fonctions qui sont exécutées par le sous-système 61, on indiquera que le mécanisme de manipulation des cartes de crédit répond à une commande de direction et de déplacement de la carte de crédit en actionnant un moteur qui entraîne un système d'entraînement des cartes de façon à déplacer la carte de crédit sous une tête de lecture. Des détecteurs (interrupteurs ou cellules photoélectriques) sont disposés pour détecter la présence de la carte de crédit dans une position d'entrée (1), dans la position de coïncement à la sortie (2) et dans la position d'attente de réalisation de transaction de la carte (3). Lorsqu'un détecteur est actionné, un bit d'information est disponible dans un mot d'état pour indiquer cette condition. Lorsque le microprocesseur 72 lit périodiquement les divers mots d'état au cours d'une opération de lecture, il détermine si la carte de crédit a atteint la zone d'attente de transaction dans laquelle la carte est retenue. Le processeur 72 commande alors l'inversion du moteur d'entraînement de la carte de crédit pendant une courte période de temps pour "freiner" puis commande l'arrêt du moteur. D'une manière élémentaie similaire, le sous-système commande la totalité des opérations de traitement de la carte de crédit telles que la retenue de la carte ou son retour à l'utilisateur. D'autres fonctions comportent la commande du dispositif de réception des dépôts dans lequel l'utilisateur peut déposer des documents qui sont transférés à une boite de retenue d'une manière telle que l'utilisateur n'a jamais accès à la boite de retenue. D'une manière similaire, le sous-système commande l'ouverture et la fermeture des portes d'accès des utilisateurs et la délivrance de montants prédéterminés en espèces à une zone d'attente de transaction dans laquelle des états de transaction imprimés peuvent également être conservés avec les espèces et la délivrance ou la retenue des documents présentés à la zone d'attente de transaction. En plus de la détection de l'état des organes mécaniques qui sont actionnés par le sous-système 61, ce dernier détecte la présence d'espèces mises en réserve dans le dispositifde délivrance d'espèces et émet un signal d'avertissement lorsqu'il n'y a pas suffisamment d'espèces disponibles pour exécuter

une transaction de délivrance d'espèces. Le sous-système 61 détecte également plusieurs conditions qui peuvent être communiquées à un panneau de télécommande ainsi qu'au microprocesseur 72. Les signaux transmis à distance comprennent notamment des signaux indiquant si la porte de service est ouverte, si une grille de détection de pénétration a été dérangée et si une condition "intervention requise" existe ou non. D'autres signaux qui peuvent être transmis au panneau de télécommande sont notamment le signal d'indication d'épuisement des formulaires d'état de transaction ou des espèces, le signal d'indication d'ouverture de la porte de service dont l'accès est réservé à l'opérateur, le signal indiquant que le système est prêt pour l'établissement de communications entre le terminal et le processeur. Le panneau de commande peut comporter des interrupteurs de restauration du terminal et un interrupteur d'essai en boucle qui commande un essai de la voie de communication.

V- Sous-système de communication avec l'utilisateur

Un sous-système de communication avec l'utilisateur 62 commande des communications bidirectionnelles entre le terminal 14 et un utilisateur. Le sous-système 62 comporte un clavier pour recevoir les commandes engendrées par l'utilisateur, un dispositif d'affichage constitué par un tableau de 222 points horizontaux sur 7 points verticaux et comporte un circuit logique de commande d'affichage et une mémoire tampon de régénération. Le circuit logique de commande d'affichage reçoit "l'image par points" des données particulières à afficher puis continue ensuite à les afficher jusqu'à réception d'une commande contraire.

Le clavier est divisé en plusieurs parties comportant chacune un certain nombre de touches. Par exemple, une partie de sélection de transaction indique le type de transaction qu'un utilisateur désire exécuter. Les autres parties sont notamment la partie de sélection du compte débité indiquant un compte sur lequel les fonds doivent être prélevés. La partie de sélection de compte "crédité" indiquant un compte auquel les fonds doivent être déposés et une partie de clavier numérique permettant l'entrée de chiffres décimaux, tels que les numéros d'identification personnels ou des montats en francs. Des lampes, d'éclairage de fond sont prévues sous les touches de sélection de fonction, de compte débité et de compte crédité pour engendrer une représentation récapitulative de vérification afin d'indiquer à un utilisateur quelles sont les touches qui ont été sélectionnées dans les parties du clavier précédemment utilisées. Toutes les lampes d'éclairage de fond sont éclairées dans la partie du clavier dans laquelle se trouve la touche qui doit être ensuite actionnée. Par exemple, lorsqu'un utilisateur insère sa carte de crédit dans le terminal 14, il est invité à frapper son numéro d'identification personnel. Après réception convenable du numéro d'identification,

toutes les touches de la zone de sélection de fonction sont alors allumées. Lorsque l'utilisateur actionne une touche particulière, telle que la touche de transfert de fonds, les autres lampes d'éclairage s'éteignent et seule la touche de transfert de fonds reste allumée. Toutes les touches de la partie de clavier suivante, telle que la partie de "compte débité" sont alors éclairées en préparation de l'étape suivante de la demande de transaction. De cette manière, une représentation récapitulative de vérification est affichée pour indiquer les sélections précédemment effectuées et la partie de sélection suivante est également indiquée. Des messages affichés et des codes de couleurs peuvent être également utilisés pour guider l'utilisateur afin qu'il exécute les opérations suivant la séquence appropriée. Le circuit logique de commande du clavier du sous-système 62 comporte les circuits nécessaires pour éclairer par-dessous les touches spécifiques commandées par le microprocesseur 72 et pour indiquer au microprocesseur quelles sont les touches qui ont été actionnées par un utilisateur.

VI - Distributeur d'états de transaction

Un sous-système distributeur d'états de transaction 63 comporte un dispositif de manipulation de formulaires pour entraîner les formulaires d'état de transaction, une imprimante, un circuit logique de commande de l'imprimante et un circuit logique d'interface pour établir la jonction du sous-système 63 avec le bus 52. Le sous-système distributeur d'états de transaction 63 n'effectue que des commandes de base spécifiques, telles que le déplacement de départ ou l'impression de caractères spécifiques. Le sous-système recueille les informations sur l'état physique du matériel distributeur d'états de transaction en vue de leur transmission, par l'intermédiaire du bus 52, au microprocesseur 72. Ces informations sont alors utilisées par le microprocesseur 72 qui fonctionne sous la commande du programme pour détecter l'achèvement réussi d'une fonction élémentaire particulière et commande la mise en route d'autres fonctions.

VII - Sous-système des fonctions assurées par l'opérateur

Un sous-système des fonctions assurées par l'opérateur 64 constitue l'interface nécessaire pour l'entretien assuré par l'opérateur et comporte des interrupteurs d'entrée, un affichage hexadécimal à quatre chiffres, un circuit de détection du courant, une mémoire auxiliaire (protégée en cas d'arrêt du courant) de 128 octets qui est utilisée pour conserver en mémoire les paramètres du système et consigner les informations exceptionnelles. Les paramètres conservés en mémoire sont, notamment, le nombre indiqué par un compteur d'espèces, les clés de chiffrement ou un numéro de transaction. L'accès au panneau de l'opérateur s'effectue par une porte à double verrouillage située à l'arrière du terminal 14 qui doit être fermée pour

qu'une opération puisse être effectuée par un utilisateur. L'ouverture de la porte d'accès et la tentative d'exécuter une fonction d'entretien provoque la destruction des clés de chiffrement qui sont normalement mises en mémoire dans cette mémoire auxiliaire. La destruction des clés assure la sécurité des clés vis à vis d'un opérateur qui pourrait chercher à utiliser des instruments électroniques pour lire la clé dans la mémoire permanente. Les clés doivent être ensuite réentrées au moyen du clavier par une personne de confiance avant que le terminal puisse être ré-ouvert. Chacune des clés de 8 octets est entrée sous forme de 16 chiffres hexadécimaux, les chiffres étant entrés deux par deux. Seuls les deux chiffres précédents sont affichés pendant que les clés sont entrées pour accroître la difficulté qu'aurait une personne non habilitée à découvrir les clés. Alternativement, une clé A qui définit la correspondance entre les numéros de compte et les numéros d'identification personnels peut être l'objet d'une protection encore plus grande en prévoyant que l'on doit entrer la clé A "déchiffrée" (clé A') qui est alors chiffrée conformément à une quatrième clé de chiffrement pour produire la clé A effective. En utilisant cette technique, la clé A effective peut rester à l'abri de tout déchiffrage par le personnel situé à l'emplacement matériel du terminal 14. Le circuit de détection du courant surveille à la fois le niveau de tension du courant alternatif du secteur et les niveaux des courants continus internes et, dans le cas où il indique que le courant alternatif est coupé et que les niveaux de tension en courant continu sont faibles mais encore utilisables, un signal est transmis du microprocesseur 72 qui sauvegarde les informations critiques, et limite l'accès à la mémoire auxiliaire tandis que cette mémoire est commandée par une source de courant auxiliaire. Un signal indicateur est transmis au panneau de l'opérateur tant que les tensions logiques en courant continu sont convenables.

VIII - Sous-système de transmission

Un sous-système de transmission 65 assure l'interface de transmission entre un canal de communication et le bus d'informations 52. Le sous-système de transmission 65 est de nature classique et reçoit des informations ou transmet des informations au bus d'informations du terminal 52, octet par octet.

IX - Connecteur de télécommande

Un connecteur de transmission de signaux à distance 70 permet la connexion de certaines lignes de signaux d'état et de certaines lignes d'entrée de signaux de commande à un panneau de télécommande qui, en fait, fait partie du terminal 14. Par exemple, une succursale de banque peut avoir cinq terminaux 14 et un unique panneau de télécommande central muni d'affichages optiques

et d'interrupteurs de commande pour chacun des cinq terminaux 14, situé en un emplacement centralisé approprié. Ces signaux transmis à distance servent principalement à la surveillance du fonctionnement des terminaux ou à la commande de conditions spéciales et ne sont pas utilisées pour les transactions d'utilisateurs normales. Le panneau de télécommande particulier utilisé a été précédemment décrit.

X - Format de messages de communication

Il existe essentiellement deux types différents de messages qui peuvent être transmis par un terminal 14 à un ordinateur 12 et quatre types de messages qui peuvent être transmis par l'ordinateur 12 à un terminal de transactions 14. Les messages du terminal à l'ordinateur comprennent un message de demande de transaction qui est le premier message de communication normal à la suite d'une demande de transaction entreprise par un utilisateur, et un message d'état qui est, le dernier message d'une séquence de trois messages. Il y a deux types de messages d'état. Le premier est un message d'état en réponse qui sert de troisième message de communication dans une séquence de transaction d'utilisateur normale et informe l'ordinateur de l'achèvement ou de l'annulation d'une transaction demandée par un utilisateur. Le second est un message d'état d'exception qui indique un état ou une condition d'un terminal 14 autre qu'une condition de fonctionnement normale. Par exemple, un message d'état d'exception sera transmis en réponse à une commande d'interrogation de l'ordinateur, si la porte d'entretien est ouverte, à la suite de la détection d'une condition d'erreur grave, telle que le coincement de la porte des utilisateurs ou une panne du matériel, ou chaque fois qu'une initialisation est nécessaire.

Les quatre types de messages qui peuvent être transmis par un ordinateur 12 à un terminal de transaction 14 sont un message de réponse de transaction, un message de commande, un message de chargement d'initialisation et un message d'écho. Le message de réponse de transaction est la réponse normale à un message de demande de transaction et informe le terminal 14 de la manière suivant laquelle la transaction demandée doit être exécutée. Un message de commande commande l'exécution de modification apportée à l'état logique d'un terminal 14 et peut également servir d'interrogation pour un message d'état si aucun changement n'est désiré. Un message de chargement d'initialisation est transmis par l'ordinateur à un terminal 14 en réponse à un message d'état d'exception demandant l'initialisation (procédure de chargement initial). Le message de chargement d'initialisation contient un texte de message, des informations de sélection d'options, des tables de caractères, des routines de programmes et d'informations de données destinées à être mises en mémoire dans la partie à accès sélectif de la mémoire

de données 74 du microprocesseur 72 du contenu dans un terminal 14. Un message d'écho est utilisé en tant qu'essai et diagnostic et ne peut être transmis que lorsqu'un terminal 14 est à l'état fermé. Le terminal 14 répond à un message d'écho par un message d'écho.

Il n'existe que trois séquences de messages de base qui peuvent être utilisées pour la communication de messages entre un terminal 14 et un ordinateur 12. Une séquence à un seul message est constituée par un message d'état d'exception transmis par un terminal 14 à l'ordinateur 12. Le message d'état d'exception peut indiquer qu'une condition anormale s'est produite ou peut être une demande d'initialisation. Un "message de commande" du processeur n'est pas nécessaire. Le contenu du message indique quel est le cas.

Une séquence de deux messages peut comporter soit un message de commande ou un message de chargement d'initialisation du processeur 12 à un terminal 14 suivi d'un message d'état approprié du terminal 14 à l'ordinateur 12, soit un message d'écho de l'ordinateur suivi d'un message d'écho du terminal. Le terminal de transaction 14 rejette une commande qui est reçue pendant que le terminal est en train de traiter une commande antérieure, un message initelligible ou un message de réponse de transaction non demandée. Dans chaque cas, l'ordinateur peut être soit un ordinateur éloigné soit un ordinateur local directement connecté.

Chaque fois que le terminal 14 est mis dans la condition de mise sous tension initiale, pour quelque raison que ce soit, le terminal 14 doit demander et recevoir un message de chargement d'initialisation de l'ordinateur avant qu'il puisse être réouvert pour accepter des transactions. Les terminaux de transactions, tels que les terminaux 36, 44 et 46 de la figure 1, qui sont connectés à une unité de commande 32 peuvent fonctionner dans un mode autonome. Dans de telles circonstances, l'unité de commande 32 sort d'ordinateur hôte et enregistre simplement les transactions d'utilisateurs, par exemple sur un disque ou une bande magnétique. Les informations des transactions sont ensuite mises à la dispositio d'un système de comptabilité des transactions à un moment ultérieur pour permettre la mise à jour des comptes. Si les terminaux fonctionnent dans le mode connecté ou en groupe, certaines fonctions de l'ordinateur peuvent être remplies par l'unité de commande 32, telles que la mise en mémoire du programme d'initialisation pour les terminaux mais, normalement, toutes les communications sont simplement transmises à l'ordinateur 12 sans changement. Dans un tel mode de fonctionnement connecté, l'ordinateur 12 peut mettre à jour les registres de comptes dans son fichier central en temps réel, c'est-à-dire au moment où les transactions demandées par les utilisateurs sont exécutées.

Chaque fois qu'un terminal 14 cesse d'être alimenté en courant, les informations de la partie à accès sélectif de la mémoire de données 66 sont perdues et l'initialisation doit être demandée au moment de la remise sous tension. Après réception des informations d'initialisation de l'ordinateur hôte, un terminal 14 peut être ouvert pour recevoir des transactions d'utilisateurs mais seulement sur ordre de l'ordinateur hôte. L'initialisation est effectuée par un terminal 14 en transmettant un message d'état d'exception demandant l'initialisation. L'ordinateur commence alors une nouvelle séquence de communications en transmettant un message d'initialisation (en plusieurs parties) contenant les informations d'initialisation demandées. Après avoir reçu de façon satisfaisante les informations d'initialisation, le terminal demandeur 14 achève la séquence de messages en retournant un message d'état à l'ordinateur hôte.

Tous les messages qui sont transmis entre un terminal de transactions 14 et un ordinateur 12 commencent par une zone d'en-tête de quatre octets. L'octet 1 de la zone d'en-tête est un octet de longueur de message (L) qui contient un compte binaire du nombre des octets contenus dans le texte du message (y compris l'octet de longueur L). L'octet 2 est un numéro de série de transaction (N), d'un octet, sous forme binaire. Ce numéro est incrémenté pour chaque nouvelle transaction d'utilisateur et est inclus dans tous les messages échangés pour cette transaction. Ce numéro est compris entre 1 et 255 ixclusivement. La valeur zéro (valeur héxadécimale 00) est utilisée pour les messages qui ne se rapportent pas à une transaction d'utilisateur. Ainsi, le compteur du nombre des transactions, qui est incrémenté à chaque nouvelle transaction d'utilisateur passe, lorsque sa capacité est dépassée, de la valeur héxadécimale FF à la valeur héxadécimale 01. Le numéro de transaction (N) est mis en mémoire dans la mémoire auxiliaire protégée du sous-système des fonctions assurées par l'opérateur 64 de sorte qu'il reste disponible après une coupure de courant de faible durée. L'octet 3 de la zone d'en-tête commune est un octet de classe (C) qui identifie le type du message et, ainsi, le format du message qui est transmis. L'octet 4 est l'octet final de la zone d'en-tête et identifie la sous-classe du message (SC) qui sert de modificateur à l'octet de classe de message.

Seul un petit nombre de combinaisons possibles de classes de messages (C) et de sous-classes de message (SC) est en fait utilisé. La classe 01 identifie un message de demande de transaction d'un terminal 14 à l'ordinateur hôte. Dans la classe 01 neuf sous-classes sont utilisées. La sous-classe désignée par la valeur héxadécimale 00 indique qu'une transaction demandée par un utilisateur est incomplète du fait que le numéro d'identification n'a pas été convenablement entré. La sous-classe désignée par

la valeur hexadécimale 01 indique une demande de délivrance d'espèces. La sous-classe désignée par la valeur hexadécimale 02 indique une demande d'informations sur le compte. La sous-classe désignée par la valeur hexadécimale 03 indique qu'un utilisateur demande à déposer des fonds. La sous-classe désignée par la valeur hexadécimale 04 indique qu'un utilisateur demande le transfert de fonds d'un compte à un autre. La sous-classe désignée par la valeur hexadécimale 05 indique qu'un utilisateur demande à payer un emprunt ou un effet en déposant de l'argent liquide dans le terminal de transaction. La sous-classe désignée par la valeur hexadécimale 06 indique une transaction spéciale, dans laquelle la nature de la transaction est identifiée par l'entrée d'un numéro prédéterminé sur le clavier et non par l'actionnement d'une unique touche dans la partie de sélection de transactions du clavier. La sous-classe désignée par la valeur hexadécimale 07 indique que la transaction demandée est incomplète du fait que le volet de dépôt recouvrant la boite de dépôts a été forcé. La sous-classe désignée par la valeur hexadécimale 08 indique une demande de paiement d'un effet ou d'un emprunt par le transfert de fonds d'un compte à un autre.

Une classe de messages C désignée par la valeur hexadécimale 15 identifie un message d'état transmis par un terminal 14 à un ordinateur 12. Il existe cinq sous-classes de messages dans cette classe. La sous-classe désignée par la valeur hexadécimale 01 indique un message d'état d'achèvement de transaction. La sous-classe désignée par la valeur hexadécimale 02 indique que le message est émis en réponse à l'exécution d'une commande et le numéro de transaction N dans l'en-tête commune doit être mis à 0. La sous-classe désignée par la valeur hexadécimale 03 est un message d'état d'exception indiquant une condition d'erreur ou demandant l'initialisation et le numéro de transaction N doit être mis à 0. La sous-classe désignée par la valeur hexadécimale 04 indique que le message d'état est transmis en réponse à l'initialisation et le numéro de transaction N doit être mis à 0. La sous-classe désignée par la valeur hexadécimale 08 est un message de réponse à une demande de rétablissement ou un message de réponse à une commande et le numéro de transaction N doit être mis à 0 pour ce message. Une demande de rétablissement indique que l'ordinateur a perdu la trace de la transaction en cours et demande une mise à jour.Le terminal répond par un message d'état d'exception.

Un message de réponse de transaction d'un ordinateur hôte à un terminal de transactions 14 est indiqué par la classe désignée par la valeur hexadécimale 0B. Il y a 9 sous-classes indiquées par l'octet de sous-classe dans cette classe. La sous-classe désignée par la valeur hexadécimale 00 indique que la transaction est incomplète du fait que le numéro d'identification

n'a pas été convenablement entré. La sous-classe désignée par la valeur hexadécimale 01 indique une demande de transaction de délivrance d'espèces. La sous-classe désignée par la valeur hexadécimale 02 indique une demande de transaction d'interrogation sur un compte. La sous-classe désignée par la valeur hexadécimale 03 indique une demande de transaction de dépôt. La sous-classe désignée par la valeur hexadécimale 04 indique une demande de transaction de transfert de fonds dans laquelle des fonds doivent être transférés d'un compte à un autre. La sous-classe désignée par la valeur hexadécimale 05 indique une demande de transaction pour le paiement d'un emprunt ou d'un effet par un transfert de fonds déposés dans le terminal à un compte. La sous-classe désignée par la valeur hexadécimale 06 indique une transaction spéciale à sélection facultative dans laquelle la nature de la transaction est déterminée conformément à un numéro entré au moyen du clavier numérique et non par l'actionnement d'une touche unique dans la partie de sélection de transaction de clavier d'utilisateur. La sous-classe désignée par la valeur hexadécimale 07 indique que le message se rapporte à une transaction d'utilisateur demandée qui est incomplète du fait que le volet de la boîte de dépôt du terminal 14 a été forcé. La sous-classe désignée par la valeur hexadécimale 08 indique une transaction d'utilisateur dans laquelle un emprunt ou un effet doit être payé par un transfert de fonds d'un compte à un autre.

La classe désignée par la valeur hexadécimale 0C identifie un message de commande de l'ordinateur à un terminal 14. Un message de commande ne se rapporte pas à une transaction particulière et par conséquent le numéro de transaction N de la zone d'en-tête est toujours mis à 0. La sous-classe désignée par la valeur décimale 01 indique une commande d'ouverture. La sous-classe désignée par la valeur hexadécimale 02 indique une commande de fermeture du terminal de transactions 14. La sous-classe désignée par la valeur hexadécimale 03 indique un type de message d'interrogation pour lequel le terminal de transaction 14 n'a pas à remplir une fonction quelconque en réponse à la commande mais doit répondre par un message d'état. La sous-classe désignée par la valeur hexadécimale 04 indique une commande de changement de la troisième clé (clé B) qui est la clé de chiffrement de transmission, de la valeur courante à une valeur contenue dans le message. La sous-classe désignée par la valeur hexadécimale 05 indique une commande pour établir la clé de chiffrement de transmission en utilisant une clé auxiliaire (clé C). La sous-classe désignée par la valeur hexadécimale 06 indique qu'un terminal de transactions 14 reçoit la commande de demander l'exécution d'une procédure de chargement initial. La sous-classe désignée par la valeur hexadécimale 07 indique que le message comporte une commande

de changement de l'affichage optique ou contient un message écrit qui doit être imprimé par le distributeur d'états de transaction. La sous-classe désignée par la valeur hexadécimale 08 est une commande donnant l'ordre au terminal 14 de retransmettre un message de demande de rétablissement (sous-classe désignée par la valeur hexadécimale 08 de la classe désignée par la valeur hexadécimale 15) à l'ordinateur.

Le message de programme de chargement initial de l'ordinateur à un terminal de transaction est indiqué par la classe désignée par la valeur hexadécimale 0D qui ne comporte qu'une sous-classe désignée par la valeur hexadécimale 01.

Un message d'écho transmis par l'ordinateur au terminal 14 est indiqué par la classe désignée par la valeur hexadécimale 10. Cette classe comprend quatre sous-classes de message d'écho. La sous-classe désignée par la valeur hexadécimale 00 est un message d'écho de base et commande simplement au terminal de transaction 14 de retransmettre le message d'écho en retour à l'ordinateur. La sous-classe désignée par la valeur hexadécimale 01 indique une commande de message d'écho enregistré qui est à la fois contrôlé en ce qui concerne sa configuration binaire et reproduit. Les octets des données du texte enregistré sont choisis de façon à transmettre toutes les configurations binaires possibles pour contrôler le fonctionnement des voies de communication. La configuration de message est conservée par le terminal en vue d'une comparaison avec une seconde transmission de la configuration de message. Une sous-classe d'enregistrement variable d'écho désignée par la valeur hexadécimale 02 est similaire à la sous-classe d'écho enregistré à cette exception près que le message peut contenir des données entrée par l'ordinateur. Le terminal de transaction répète le message en retour et conserve également le message en mémoire en vue d'une comparaison avec une seconde transmission du même message. A la suite de la réception de la seconde transmission du message, le terminal de transaction contrôle le message et le retransmet comme dans le cas de la sous-classe 01. Un message de demande de données consignées est indiqué par la sous-classe désignée par la valeur hexadécimale 03. Ceci provoque la transmission par le terminal des 8 enregistrements de consignation d'erreurs les plus courantes. Aucun chiffrement ni déchiffrement n'est nécessaire pour la transmission des messages d'écho quels qu'ils soient.

La zone d'en-tête commune de quatre octets de chaque message est suivie par les données du message dans un format qui dépend du type particulier de message qui est transmis. Pour un message de demande de transaction transmis par le terminal 14 à l'ordinateur, les octets 1 à 4 de l'en-tête commune sont suivis des octets 5 à 8 qui contiennent une zone chiffrée

de 32 bits. Cette zone chiffrée de 32 bits sera décrite en plus de détails ci-après mais, considérée d'une manière générale, cette zone comporte une forme "chiffrée" du numéro d'identification personnel qui a été entré au moyen du clavier des utilisateurs et un octet d'informations variables qui peut être soit le contenu d'un compteur d'espèces soit le contenu d'un compteur du nombre des transactions effectuées.

L'octet 9 est un octet de sélection du compte débité (FAS) indiquant celle des touches de la partie de sélection du compte débité du clavier des utilisateurs qui a été actionnée. Le contenu des données de ce neuvième octet indique le compte d'où les fonds nécessaires pour la transaction demandée par l'utilisateur doivent être prélevés. La valeur hexadécimale 21 indique que le compte débité est un compte courant, la valeur hexadécimale 22 qu'il s'agit d'un compte d'épargne, la valeur hexadécimale 23 qu'il s'agit d'un compte de carte de crédit et la valeur hexadécimale 24 indique qu'il s'agit d'un compte spécial à sélection facultative qui est plus complètement défini par un modificateur numérique. En effectuant des arrangements spéciaux avec la banque, un utilisateur peut ouvrir des comptes multiples. Des numéros prédéterminés à trois chiffres (décimaux) peuvent être alors attribués à ces comptes. En actionnant la touche de sélection facultative spéciale de la partie de compte débité du clavier, l'utilisateur est alors autorisé à entrer un numéro comportant jusqu'à trois chiffres décimaux au moyen du clavier numérique pour indiquer celui des comptes prédéfinis, qui peuvent être éventuellement nombreux, qu'il désire débiter. Ce numéro d'identification de compte est transmis un chiffre par octet plus les octets 10 et A, dans lesquels A peut avoir la valeur 10, 11 ou 12, selon que le numéro de compte spécial déterminé au moyen du clavier contient respectivement 1, 2 ou 3 chiffres. Du fait que la zone FAS (sélection de compte débité) peut avoir une longueur variable elle doit être suivie d'un octet séparateur de zones (FS) ayant la valeur hexadécimale FE qui est utilisé pour définir les limites des zones de longueur variable. Des séparateurs de zones adjacents indiquent une longueur nulle ou zone sans entrée entre eux. L'octet FS délimite la fin de la zone précédente.

A la suite de l'octet FS délimitant la zone de sélection de compte débité (FAS) se trouve une zone de sélection de compte crédité (TAS) identifiant une touche actionnée dans la partie de sélection du compte crédité du clavier des utilisateurs. La valeur hexadécimale 31 indique que le dépôt doit être sur un compte-chèque, la valeur hexadécimale 32 sur un compte épargne, la valeur hexadécimake 33 à un compte de carte de crédit et la valeur hexadécimake 34 indique un renvoi à une touche spéciale de sélection de compte crédité qui peut être modifiée par une valeur comportant jusqu'à trois chiffres

(décimaux) entrés immédiatement après le premier octet TAS. Ces modifications numériques ont la même signification dans la zone TAS que dans la zone FAS. Du fait que la zone TAS a une longueur variable, elle doit être également suivie d'un octet FS séparateur de zones contenant la valeur hexadécimale FE. A la suite de l'octet séparateur de zones pour la zone de sélection de compte crédité, les données qui sont lues sur la bande magnétique de la carte de crédit sont transmises. En retirant le bit de parité du code normalisé de l'American Bankers Association, il est possible de comprimer deux caractères de quatre bits de données de la carte de crédit dans chaque octet du message. Dans le cas où un nombre impair de caractères de carte de crédit apparait sur la carte de crédit, le dernier octet est rempli par la valeur hexadécimale F pour remplir tous les octets du message. Le début des caractères de la carte, la fin des caractères de la carte et les caractères de contrôle longitudinaux par redondance (LRC) sont exclus du message de demande de transaction transmis étant donné qu'ils sont contrôlés par le terminal 14.

Les positions d'octets 5 à 8 de la zone d'entrée contiennent une zone chiffrée de 32 bits. Cette zone de 32 bits sera décrite de façon plus détaillée ci-après mais elle comporte, d'une manière générale, une répétition du numéro de transaction (N), huit bits qui représentent le compte d'espèces tournant pour la coupure ou billet de banque N°2 (CNTR2) huit bits indiquant le nombre d'octets d'état (CB) et huit bits représentant le compte d'espèces tournant pour la coupure ou billet de banque N°1 (CNTR1). L'octet CB est une zone d'un octet contenant un compte binaire du nombre des octets de données d'état et d'interrogation qui suivent la partie chiffrée (octets 5 à 8) du message pour un message d'état normal. Pour un "message de rétablissement de demande", la zone CB contient la "zone d'action" de la réponse de transaction pour le dernier message de demande de transaction. La zone d'action est une zone de 8 bits transmise en tant que partie de la zone chiffrée de 32 bits d'un message de réponse de transaction. Les parties de compteurs de huit bits (CNTR) de la zone chiffrée de 32 bits indiquent le compte binaire des billets de banque délivrés par le premier et par le second mécanismes de délivrance d'espèces. Ces nombres sont prélevés de compteurs qui sont incrémentés pour chaque billet ou rouleau de pièces de monnaie délivré et retombent de la valeur hexadécimale FF à la valeur hexadécimale 00. Les comptes sont mis en mémoire dans la mémoire auxiliaire du sous-système 64 de sorte que ces comptes sont conservés en cas d'interruption de courte durée du courant. A la suite de la zone chiffrée de 32 bits contenue dans les octets 5 à 8 se trouve une zone de données. La zone de données comporte une zone d'état de quatre octets, dans les positions d'octets

9 à 12. Ces quatre octets définissent l'état en cours d'un terminal 14 comme décrit ci-après. La plupart des messages d'état se terminent par un octet FS à la position d'octet 13. Cependant un message d'état qui est transmis en réponse à un message de commande d'interrogation contient 112 des 128 octets mis en mémoire dans la mémoire auxiliaire du sous-système 64 qui sont transmis après les quatre octets d'état. Pour ce message, la zone CB contient le nombre 116. Les 16 octets de la mémoire permanente qui ne sont pas transmis en réponse à un message d'interrogation sont les deux clés de chiffrement de 8 octets chacune. Si le message d'état est retransmis à nouveau en réponse à un message de rétablissement de demande, les quatre octets d'état contiennent les quatre octets du dernier message d'état de transaction et sont suivis par le message de demande de transaction d'origine complet. Ces informations permettent alors à l'ordinateur de reconstituer les conditions qui existaient avant l'évènement qui a amené l'ordinateur à demander un rétablissement.

Les 32 positions binaires des quatre octets d'état, dans les positions d'octets 9 à 12 d'un message d'état, ont chacune une signification prédéterminée. Ces significations sont attribuées pour définir l'état physique et de fonctionnement d'un terminal 44 avec une précision détaillée pour qu'un ordinateur hôte puisse déterminer et commander le fonctionnement général de chaque terminal 14. Ces significations sont décrites ci-après sous la forme d'un tableau dans lequel le nombre de gauche indique le numéro de l'octet d'état, compris entre 0 et 3, l'octet d'état 0 étant dans la position d'octet 9 du message d'état et l'octet d'état 3 étant dans la position d'octet 12 du message d'état. Chaque octet d'état comporte 8 bits désignés bit 0 à bit 7, le bit 0 étant dans la position binaire la plus significative et le bit 7 dans la position binaire la moins significative.

| Octet | Bit | Description |
|---|---|---|
| 0 | 0 | bit d'état d'achèvement de transaction. Cette position binaire est mise à 1 au début de chaque transaction pour indiquer que la transaction n'a pas été achevée du fait qu'un message de réponse de transaction est nécessaire. Cette position binaire est remise à 0 lorsqu'une transaction a été exécutée de la façon spécifiée dans un message de réponse de transaction. |

| Octet | Bit | Description |
|---|---|---|
| 0 | 1 | bit de numéro de transaction invalide dans le message de réponse de transaction. Cette position binaire est remise à 0 chaque fois qu'une nouvelle transaction est commencée. Cette position binaire est mise à 1 chaque fois que le numéro de transaction (N) dans la zone d'en-tête commune d'un message reçu de l'ordinateur hôte est incorrecte. Une exception est faite dans le cas d'un message d'écho qui ne transmet pas d'informations significatives dans la position de numéro de transaction d'en-tête. |
| 0 | 2 | bit de sous-classe de transaction invalide dans le message de réponse. Cette position binaire est remise à 0 chaque fois qu'une nouvelle transaction est commencée et est mise à 1 chaque fois qu'un message de réponse de transaction est reçu qui contient dans le quatrième octet, ou octet de sous-classe, de la zone d'en-tête commune un nombre différent de celui du message de demande de transaction. La position binaire 0 de l'octet 0 doit être mise à 1 en même temps que cette position binaire. |
| 0 | 3 | bit de classe invalide. Cette position binaire est remise à zéro après qu'un message d'état d'exception a été transmis et mise à 1 chaque fois qu'un message est reçu de l'ordinateur hôte et contenant une désignation de classe invalide dans l'octet 3 de la zone d'en-tête commune. A titre d'exemple, un terminal 14 peut recevoir un message d'initialisation (IPL) non demandé ou un message de réponse de transaction non demandé. |
| 0 | 4 | bit d'erreur du montant dans le message de réponse de transaction. Cette position binaire est remise à 0 au début de chaque nouvelle transaction et mise à 1 chaque fois qu'un message de réponse de transaction est reçu dont l'octet de montant en francs dans sa zone chiffrée indique un montant incorrect (AMT). le bit 0 de l'octet 0 doit être mis à 1 chaque fois que cette position binaire est mise à 1. |
| 0 | 5 | non affecté. |

| Octet | Bit | Description |
|---|---|---|
| 0 | 6 | bit de transaction annulée par le client. Cette position binaire est remise à 0 au début de chaque nouvelle transaction et mise à 1 dans le cas où un client actionne une touche d'annulation sur le clavier des utilisateurs à la suite de la transmission de la transaction d'un message de demande de transaction. |
| 0 | 7 | bit d'expiration du tems de l'utilisateur. Cette position binaire est remise à 0 au début de chaque bnouvelle transaction d'utilisateur et mise à 1 chaque fois qu'un utilisateur utilise une période de temps supérieure à une période de temps allouée pour entrer un numéro au moyen du clavier des utilisateurs ou pour déposer des objets par la trappe de dépôt. Le bit 0 de l'octet 0 doit être mis à 1 chaque fois que cette position binaire ou la position binaire 0 6 est mise à 1. |
| 1 | 0 | bit de rejet de commande. Cette position binaire est remise à 0 après qu'un message d'état en réponse à une commande a été transmis. Cette position binaire est mise à 1 à la réception d'un message de commande qui ne peutpas être exécuté du fait que le terminal 14 est occupé au moment où une commande est reçue. |
| 1 | 1 | bit de commande invalide. Cette position binaire est remise à 0 à la suite de la transmission d'un message d'état en réponse à une commande. Cette position binaire est mise à 1 chaque fois qu'un message de commande est reçu dans lequel des zones sont manquantes. Par exemple, une commande de changement de clé qui ne comporte pas la nouvelle clé ou une commande de changement d'affichage sans une nouvelle zone d'affichage. Cette position binaire est également mise à 1 en réponse à un message de commande contentant une désignation de sous-classe invalide dans l'octet 4 de la zone d'en-tête commune. |
| 1 | 2 | bit de demande de procédure de chargement initial (IPL). Cette position binaire est remise à 0 à la suite de la réception convenable d'un message |

| Octet | Bit | Description |
|---|---|---|
| | | de chargement d'initialisation de l'ordinateur hôte et mise à 1 chaque fois qu'un terminal 14 passe de l'état fermé à l'état ouvert, par exemple, à la suite de la fermeture du panneau d'accès de l'opérateur inspecteur ou à la suite d'une commande de l'ordinateur hôte. Ce bit est également à 1 chaque fois qu'un terminal 14 reçoit un message de commande commandant au terminal de demander une procédure de chargement initial. bit de procé |
| 1 | 3 | bit de procédure de chargement initial et de processus en cours. Cette position binaire sert de bit modificateur des bits 2 et 3 égale à 00 indique que le terminal est initialisé. Cette condition ne peut se reproduire que lorsque le terminal est à l'état ouvert. La combinaison des bits 2 et 3 égale à 10 indique que l'initialisation a été demandée mais que le message de chargement d'initialisation n'a pas été reçu. Une combinaison des bits 2 et 3 égale à 11 indique qu'un chargement d'initialisation est en cours. |
| 1 | 4 | bit d'erreur du compteur d'espèces. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est mise à 1 chaque fois qu'un message de réponse de transaction est reçu qui contient un octet de compteur d'espèces (CNTR) dans sa zone chiffrée qui ne correspond pas à l'état du compteur d'espèces situé dans le terminal. Le compteur d'espèces est un compteur en anneau qui est incrémenté chaque fois qu'un nouveau billet est délivré. Le bit 0 de l'octet 0 doit être mis à 1 chaque fois que cette position binaire est mise à 1. |
| 1 | 5 | bit d'erreur de la zone de classe et sous-classe (C et SC). Cette position binaire est remise à 0 à la suite de la transmission d'un message d'état d'exception. Elle est mise à 1 à la suite de la réception d'un message de commande de l'ordinateur hôte qui contient un octet de classe et de sous-classe (C et SC) dans la zone de données chiffrées qui ne concorde pas avec l'octet de classe et de sous-classe de la zone d'en-tête commune. |

| Octet | Bit | Description |
|---|---|---|
| | | Ce défaut de concordance indique une erreur de synchronisation de la clé ou une erreur de l'ordinateur. Dans un message de commande normal, les deux octets de classe (C) et de sous-classe (SC) de la zone d'en-tête commune sont combinés en un unique octet de classe et sous-classe (C et SC) (comprimé en supprimant les quatre bits 0 de gauche de chaque octet). |
| 1 | 6 | bit d'expiration du temps de communication pour la séquence de réponse de transaction. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est mise à 1 chaque fois qu'une période de temps prédéterminée expire à la suite de la transmission d'un message de demande de transaction d'un utilisateur sans qu'un message dréponse de transaction correspondant ait été reçu. Le bit de position 0 de l'octet 0 doit être mis à 1 chaque fois que cette position binaire est mise à 1. |
| 1 | 7 | bit de message inintelligible. Cette position binaire est remise à 0 après transmission d'un message d'état d'exception. Elle est mise à 1 pour indiquer un message inintelligible chaque fois qu'un message est reçu qui ne correspond pas au format de message prédéterminé requis. Par exemple, le nombre d'octets peut ne pas concorder avec la désignation de longueur de message (L) dans l'en-tête commune ou une erreur de parité peut se produire à la suite de la lecture d'un octet de données ou une position d'octet peut contenir des données invalides. |
| 2 | 0 | bit de retenue de carte. Ce bit est remis à 0 au début de chaque nouvelle transaction d'utilisateur et est mis à 1 chaque fois qu'une transaction demandée par l'utilisateur est terminée et que le terminal 14 conserve la carte de crédit qui y a été insérée par l'utilisateur. Cette position binaire indique que la carte a été retenue par suite d'une erreur du terminal 14 et non en réponse à une commande de l'ordinateur. |

| Octet | Bit | Description |
|---|---|---|
| 2 | 1 | bit d'erreur de distribution. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est mise à la valeur logique 1 chaque fois qu'une erreur se produit au cours de la distribution d'un document tel qu'un billet ou un état de transaction. Cette position binaire est mise à l'état logique 1 chaque fois qu'un document tombe d'une zone d'attente dans une boite de retenue. Etant donné que la transaction peut être achevée après un nouvel essai, cette position binaire n'indique pas nécessairement une transaction d'utilisateur inachevée. |
| 2 | 2 | bit d'erreur irrémédiable du dispositif de dépôt. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est mise à 1 chaque fois qu'une condition d'erreur telle qu'un coïncement se produit dans le dispositif de dépôt du terminal et que le terminal est incapable de sortir de cette condition d'erreur. |
| 2 | 3 | bit de dépassement de capacité de la table d'affichage. Cette position binaire est remise à 0 à la suite de la transmission d'un message d'état. Cette position binaire est mise à 1 à la suite de la réception d'un message de commande de changement d'affichage émanant de l'ordinateur hôte qui contient plus de données d'affichage que le système d'affichage du terminal ne peut traiter. Un message d'affichage incorrect n'est pas accepté par un terminal 14. |
| 2 | 4 | non affecté |
| 2 | 5 | non affecté |
| 2 | 6 | bit d'intervention requise. Ce bit est remis à 1 lorsqu'une condition d'intervention requise se produit. Il est remis à 0 lorsque l'indicateur d'intervention requise est remis à zéro. |
| 2 | 7 | bit d'expiration du temps d'enlèvement de la carte. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est mise à 1 chaque fois qu'une |

| Octet | Bit | Description |
|---|---|---|
| | | période de temps prédéterminée expire à la suite de la mise à disposition de l'utilisateur d'une carte de crédit sans que la carte ait été retirée d'un terminal 14. Cette position binaire indique qu'un type quelconque d'intervention est requis. Normalement, l'ordinateur hôte répond en commandant au terminal de retenir la carte de crédit. |
| 3 | 0 | bit d'ouverture/fermeture. Cette position binaire est remise à 0 chaque fois que le terminal est ouvert et est prêt à recevoir une demande de transaction d'utilisateur. Cette position binaire est mise à 1 chaque fois que le terminal est fermé. |
| 3 | 1 | bit de condition d'épuisement des espèces. Cette position binaire est remise à zéro au début de chaque nouvelle transaction d'utilisateur. Cette position binaire est sensible à un interrupteur qui indique s'il y a suffisamment d'espèces en réserve dans le terminal pour exécuter une transaction de délivrance d'espèces maximale. Cette position binaire est mise à l'état logique 1 chaque fois que la condition d'épuisement des espèces se produit au cours de l'exécution d'une transaction de délivrance d'espèces précédente à laquelle le message d'état correspond. La mise à 1 de cette position binaire indique qu'une intervention est requise et provoque la fermeture du terminal. |
| 3 | 2 | bit de clé de chiffrement auxiliaire invalide. Cette position binaire est remise à 0 à la suite de la transmission d'un message d'état et est mis à 1 à la suite de la réception d'un message de commande de type changement de clé de l'ordinateur hôte qui contient une clé de chiffrement incorrecte (une clé de chiffrement incorrecte ne contient que des 0). |
| 3 | 3 | bit d'épuisement de formulaires du distributeur d'états de transaction. Cette position binaire est remise à 0 au début de chaque nouvelle transaction d'utilisateur. Elle est mise à 1 lorsqu'un détecteur d'états de transaction indique que le dernier |

| Octet | Bit | Description |
|---|---|---|
| | | formulaire d'état de transaction utilisable est délivré au cours de la dernière transaction précédente à laquelle le message d'état correspond. |
| 3 | 4 | bit de volet (porte) de la boîte de dépôt ou de la porte de délivrance ouverte. Cette position binaire est mise à 1 lorsque le volet de la boîte de dépôt ou la porte de délivrance reste ouvert alors qu'il devrait être fermé et indique que le volet ou la porte a été forcé. |
| 3 | 5 | bit de panne irrémédiable. Cette position binaire est remise à 0 après qu'un message d'état d'exception a été transmis. Cette position binaire est mise à 1 chaque fois qu'un blocage ou autre condition d'erreur est rencontré qui ne peut être corrigé, que ce soit au cours de l'exécution d'une transaction ou à tout autre moment. La mise à 1 de cette position binaire indique qu'une intervention est requise et le terminal se ferme. |
| 3 | 6 | bit de porte des clients ouverte. Cette position binaire est remise à 0 à la suite de la transmission d'un message d'état. Cette position binaire est mise à 1 lorsque la porte des clients qui donne accès au clavier des utilisateurs et au tableau d'affichage est ouverte alors qu'elle devait être fermée ce qui indique que la porte a été forcée. La mise à 1 de ce bit indique qu'une intervention est requise et provoque la fermeture du terminal. |
| 3 | 7 | bit de verrouillage de l'enceinte de sécurité. Cette position binaire est remise à 0 lorsque la porte d'accès de l'opérateur est fermée et mise à 1 lorsque la porte est ouverte. Le terminal 14 se ferme chaque fois que cette position binaire est mise à 1. |

Un message de réponse de transaction de l'ordinateur 12 à un terminal utilisateur 14 est engendré en réponse à un message de demande de transaction d'utilisateur. Le message de réponse de transaction commence par la zone d'en-tête commune de quatre octets spécifiant la longueur totale du message (L), le numéro de transaction (N), la classe du message (C) et la sous-classe du message (SC). A la suite des quatre octets de la zone d'en-tête commune se trouvent quatre octets ou 32 bits d'informations

"chiffrées", une zone de données d'affichage facultative de longueur variable, un caractère de séparation de zones (FS), une zone d'impression d'état de transaction facultative de longueur variable et un caractère de séparation de zones final (FS). La zone chiffrée de quatre octets comporte un nombre indiqué par le compteur d'espèces 2, d'un octet (CNTR2), un unique octet d'action, un nombre indiqué par le compteur d'espèces 1, d'un octet, (CNTR1) et un octet de montant (AMT) qui spécifie le nombre de billets dont le message de réponse autorise la délivrance. Le terminal 14 vérifie le montant autorisé en le comparant à la demande.

L'octet d'action est une instruction d'un octet du processeur 12 qui instruit un terminal de façon qu'il achève une transaction d'utilisateur d'une manière concordant avec son contenu de données.

Bit 0 - Lorsque le bit 0 est mis à 1, un terminal 14 a l'ordre d'afficher immédiatement un message d'affichage de terminal type qui est indiqué par la zone de données d'affichage facultative qui suit immédiatement la zone chiffrée. Jusqu'à 128 messages séparés désignés 0 à 127 sont mis en mémoire dans la mémoire de données 74 coopérant avec le microprocesseur 72. Lorsque le bit 0 de l'octet d'action est mis à 1, le terminal 14 a l'ordre d'afficher l'un de ces messages qui est indiqué par le contenu binaire de la zone d'affichage facultative d'un octet à la position d'octet 9 du message de réponse de transaction.

Bit 1 - Lorsque le bit 1 est à 1, le terminal 14 a l'ordre d'afficher immédiatement un message d'affichage facultatif contenu dans la zone de données d'affichage facultative suivant immédiatement la zone chiffrée. Lorsque le bit 1 est mis à 1, l'octet 9 au début de la zone de données d'affichage facultative contient un nombre binaire indiquant la longueur du message d'affichage en octets sans compter l'octet 9. Le message de réponse de transaction contient, immédiatement à la suite de l'octet 9, le texte du message désiré dans le code EBCDIC, chaque octet indiquant un caractère à afficher.

Bit 2 - Un un logique dans cette position binaire 2 de l'octet d'action indique que le terminal de transaction 14 a l'ordre d'imprimer des informations sur un état de transaction et que la zone des données d'impression d'état de transaction du message de réponse contient les données à imprimer dans le code EBCDIC.

Bit 3 - non défini.

Bit 4 Bit 4 - Un un logique dans le bit 4 indique qu'une transaction d'utilisateur demandée est autorisée telle que demandée.

Bit 5 - Un un logique dans cette position binaire indique qu'une carte de crédit d'utilisateur doit être retenue dans le terminal 14 tandis qu'un 0 logique indique que la carte de crédit doit être rendue à l'utilisateur.

Bit 6 - Un un logique dans cette position indique que l l'utilisateur doit donner son accord à la transaction avant que le terminal 14 poursuive l'exécution de la transaction. L'utilisateur refuse ou donne son accord à la transation en actionnant une touche d'exécution prévue dans la partie de commande du clavier. Typiquement une indication de la transaction est affichée au moment où l'utilisateur doit choisir une touche. Par exemple, le message "TRANSFERT 250F DU COMPTE EPARGNE AU COMPTE COURANT - Appuyer sur Annulation ou Poursuite" peut être affiché.

Bit 7 - Non défini.

La zone d'impression de l'état de transaction à la fin d'un message de réponse de transaction est divisée en plusieurs sous-zones, ce qui permet la communication de données d'impression pour un maximum de 2 formulaires d'état de transaction. La première sous-zone est une sous-zone de données communes qui comporte des informations telles que le nom de l'utilisateur et le numéro de compte qui sont les mêmes pour les deux états de transaction. La zone de données communes peut, soit commander à un terminal 14 d'imprimer un message d'impression enregistré mis en mémoire dans la mémoire 66, soit commander au terminal d'imprimer un message transmis en tant que partie de la zone de données communes dans le code normalisé EBCDIC. Le premier octet de la zone de données communes détermine la source des données d'impressions. Si cet octet contient un nombre compris entre 1 et 127 (inférieur à la valeur hexadécimale 80), les données d'impression sont contenues sous la forme EBCDIC normalisée dans la sous-zone de données communes immédiatement à la suite du premier octet. Dans ce cas, le premier octet représente un compte de longueur binaire indiquant le nombre d'octets du texte de la zone de données communes en dehors de l'octet de longueur. Si les données d'impression communes doivent être extraites d'un message enregistré, un numéro d'identification d'un message d'impression identifiant le message enregistré particulier est ajouté à 128 (valeur hexadécimale 80) et transmis en tant que premier et unique octet de la sous-zone de données communes. A titre d'exemple, si les données communes doivent être extraites d'un message enregistré N°30, la sous-zone de données communes d'un seul octet contient le nombre binaire 30+128 = 158 (valeur hexadécimale 9E).

Un contenu de données d'un octet correspondant au numéro d'identification 0 (valeur héxadécimale 80) est utilisé comme délimiteur entre les données communes et les données d'état et ne doit pas être utilisé pour définir un message ϕ en tant que message enregistré. Une sous-zone de données d'état N°1 suit immédiatement l'octet délimiteur de valeur héxadécimale 80 après la sous-zone de données communes. La sous-zone de données d'état N°1 peut comporter un message d'impression effectif en code EBCDIC ou peut identifier un message d'impression enregistré et utilise le même format que la sous-zone de données communes. Les informations d'impression commandées par la zous-zone de données d'état N°1 ne sont cependant imprimées que sur un formulaire d'état de transaction désignée formulaire N°1 . Le délimiteur (valeur héxadécimale 80) suit immédiatement la sous-zone de données d'état N°1. Une sous-zone de données d'état N°2 suit immédiatement le second délimiteur. La sous-zone de données d'état N°2 a un format et un contenu de données similaires à ceux de la sou-zone de données communes et de la sous-zone de données d'état N°1. La sous-zone de données d'état N°2 peut contenir soit un message d'impression transmis en code EBCDIC soit l'identification d'un message d'impression enregistré. Si la sous-zone d'état N°2 n'est pas présente, c'est-à-dire si elle a une longueur de 0 octet, il n'est ni imprimé ni délivré de second état de transaction. Un caractère de séparation de zones (FS) suit immédiatement la sous-zone de données de l'état N°2 pour indiquer la fin de la zone d'impression d'état de transaction et la fin d'un message de réponse de transaction. L'impression d'un formulaire d'état de transaction commence à l'angle supérieur gauche et se poursuit de gauche à droite suivant le format d'écriture latine courante. Un code de commande de chariot en code EBCDIC est utilisé pour terminer une ligne de texte et commencer l'impression du caractère de texte à la position de caractère d'extrême gauche de la ligne inférieure suivante. L'opération d'impression est effectuée suivant une séquence prédéterminée suivant laquelle le texte commun est tout d'abord imprimé sur le formulaire d'état N°1 , le texte de l'état N°1 est imprimé sur le formulaire d'état N°1, le texte commun est imprimé sur le formulaire d'état N°2 et enfin le texte d'état N°2 est imprimé sur le formulaire d'état N°2.

Un message de commande est transmis par l'ordinateur 12 à un terminal 14 pour commander le fonctionnement ou l'état du terminal conformément au contenu de données du message de commande. Chaque message de commande commence par une zone d'en-tête commune de quatre octets contenant la longueur du message (L), le numéro de transaction (N), la classe du message (C) et la sous-classe du message (SC). Une zone chiffrée de quatre octets suit la zone d'en-tête de quatre octets. La zone chiffrée de quatre octets comporte l'octet du premier compteur d'espèces (CNTR1), l'octet de classe et sous-classe

(C et SC) contenant les indicateurs de classe et de sous-classe combinée en un seul octet, l'octet du second compteur d'espèces (CNTR2) et un octet spécial (SPEC). L'octet spécial est utilisé pour un message de commande du type interrogation afin d'indiquer les informations qui doivent être fournies, par un message d'état en réponse d'un terminal commandé, à l'ordinateur . Les bits 0 à 4 de l'octet spécial ne sont pas affectés et sont normalement transmis sous forme de 0. Le bit 5 est mis à 1 pour indiquer que le terminal a l'ordre de retransmettre son dernier message d'état. Le bit 6 est mis à 1 pour indiquer que le terminal doit transmettre un message d'état actuel plus les 112 octets de la mémoire auxiliaire contenues dans le sous-système des fonctions assurées par l'opérateur 64 qui ne comprennent pas les deux clés de chiffrement. Un 1 dans le bit 7 de l'octet spécial indique que le terminal a l'ordre de transmettre un message d'état normal. Les bits 5, 6 et 7 sont mutuellement exclusifs de sorte qu'un seul d'entre eux doit être à l'état 1 à un moment quelconque.

Deux zones chiffrées facultatives suivent la zone d'en-tête commune et la zone chiffrées de quatre octets d'un message de commande. La première zone chiffrée facultative comporte la première moitié d'une clé de chiffrement de 8 octets et la seconde zone chiffrée facultative comporte la seconde moitié d'une clé de chiffrement de 8 octets. Ces première et seconde zones chiffrées facultatives ne sont comprises dans le message de commande qu'à la suite d'une commande d'établissement de clé ou de changement de clé. Un terminal 14 répond à une commande de changement de clé en déchiffrant le message de commande avec l'ancienne troisième clé ou clé de chiffrement de transmission (clé B) puis il lui substitue la clé, reçue dans les zones chiffrées faculatatives une et deux, dans toutes les communications ultérieures. Une commande d'établissement de clé fonctionne de la même manière qu'une commande de changement de clé à cette exception près que la nouvelle clé est déchiffrée au moyen d'une clé auxiliaire (clé C) mise en mémoire dans la mémoire auxiliaire. Dans un message de commande de type message de "changement d'affichage", les deux zones chiffrées facultatives ne sont pas prévues dans le message mais une zone de données facultative en clair suit la zone chiffrée de quatre octets. La zone de données facultatives en clair commence par un numéro d'indexation (INDX) suivi d'un octet de longueur de la zone de données (LD) et d'un nouveau texte d'affichage en code EBCDIC normalisé. Un message de commande du type message de changement d'affichage n'a pas d'effet sur l'affichage effectif que peut observer l'utilisateur du terminal mais modifie, par contre, le contenu de données d'un message d'affichage enregistré mis en mémoire dans la mémoire des données 74. Par exemple, il peut être souhaitable de changer un message enregistré tel que "retirez la carte de crédit" ayant

le numéro d'identification de message d'affichage40 par "ôter la carte de crédit". L'octet d'indexation (INDX) contient le numéro d'identification de message d'affichage du message enregistré qui doit être modifié. L'octet de longueur de la zone de données (LD) contient un nombre binaire indiquant le nombre d'octets du texte du nouveau message donné immédiatement à la suite. Si le nouveau message est trop long pour être contenu dans le nombre d'octets disponible dans la table de messages d'affichage contenu dans la mémoire de données 74, la commande n'est pas exécutée et le message d'état suivant indique que la commande n'a pas été exécutée. Du fait que les messages d'affichage ont une longueur variable et du fait qu'il est nécessaire que tous les messages de l'ordinateur à un terminal 14 contiennent un nombre pair d'octets, il peut être nécessaire de compléter la fin d'un texte d'affichage par un caractère de remplissage arbitraire. Le caractère arbitraire n'est pas compté dans l'octet de longueur totale du message (L) de la zone d'en-tête commune du message de commande.

Le message de chargement d'initialisation fournit les informations nécessaires à la partie de mémoire à accès sélectif de la mémoire de données 66 qui peuvent avoir été perdues dans le cas d'une interruption de courant. Il est également utilisé pour réinitialiser le terminal avec de nouvelles options. Ce message commence par la zone d'en-tête commune de quatre octets type suivie d'une zone contenant un nombre binaire de deux octets spécifiant le nombre d'octets de la zone de données qui suit. La zone de données comprend la dernière zone du message de chargement d'initialisation et contient l'image d'adaptation qui est mise en mémoire dans la mémoire de données 66. Les informations critiques, telles que les routines de microprogrammes et les octets de sélection d'options dans la zone de données sont chiffrées avec la troisième clé de transmission (clé B) dans des segments séquentiels de quatre octets chacun.

En général, l'image d'adaptation qui est reçue au cours de l'initialisation fournit les informations qui peuvent varier d'un terminal à un autre; il n'est par conséquent pas facile d'utiliser des mémoires mortes pour la conservation de cette image. L'image d'adaptation comporte notamment les messages enregistrés d'impression et d'affichage pour l'utilisateur qui peuvent comprendre jusqu'à 49 messages prédéterminés désignés messages 1 à 49. L'image d'adaptation comporte également, en tant que message 50, une table de caractères facultative qui contient jusqu'à 574 octets et qui permet l'affichage de caractères ou signes graphiques non normalisés qui ont été sélectés spécialement par un client de terminal donné tel qu'une banque. L'image d'adaptation comporte également une certaine quantité d'informations de programmation et de commandes de programmes pour tenir compte de la combinaison particulière d'options

disponibles qui est utilisée dans un terminal donné.

XI - Assemblage des messages de transaction

Les communications qui sont nécessaires entre un ordinateur et un terminal de transactions d'utilisateur 14 au cours de l'exécution d'une transaction demandée par un utilisateur sont représentées de façon plus détaillée dans les organigrammes des figures 3 à 5 auxquelles on se réfèrera maintenant. Afin de faciliter la compréhension du fonctionnement de l'invention, le système de communications fonctionnel sera décrit dans le contexte d'exemples de transactions d'utilisateur spécifiques. Il doit être entendu, cependant, qu'un terminal de transactions 14 peut exécuter l'une quelconque de très nombreuses transactions qui peuvent être demandées par un utilisateur et n'est pas limité à ces exemples spécifiques.

Pour la description d'un exemple spécifique, on a supposé que le terminal 14 était un terminal monté à travers un mur formant une station accessible du trottoir d'une succursale de banque. On a supposé que le terminal monté dans le mur était connecté d'une manière similaire au terminal 46 (figure 1) dans une boucle fermée aboutissant à l'unité de commande 32 et, par l'intermédiaire de l'unité de commande 32 à un ordinateur hôte 12. Le terminal 46 traverse un mur extérieur de la succursale de banque, les moyens de communication mis à la disposition des utilisateurs étant disposés à l'extérieur du terminal et la plus grande partie du terminal étant située à l'intérieur de la banque. Lorsqu'un utilisateur éventuel s'approche du terminal 46, l'éclairage de la région dans laquelle se trouve le clavier et une indication sur la face du terminal indiquent que le terminal est à l'état disponible (ouvert). L'absence d'éclairage et un affichage "fermé" indiquent que le terminal n'est pas disponible pour l'exécution de transactions et si le terminal est à l'état fermé toute action de l'utilisateur est ignorée. Si le terminal indique qu'il est à l'état ouvert, l'utilisateur éventuel commence une transaction d'utilisteur en insérant sa carte de crédit dans une fente. Dans cet exemple, on a supposé qu'un utilisateur désirait transféer des fonds de son compte épargne à un compte courant.

1.- Message de demande de transaction

La première partie de la séquence de communications de transaction d'utilisateur a été représentée sur la figure 3. Le microprocesseur 72 du terminal n'est représenté que d'une manière générale sur la figure 3, aucune connexion spécifique avec les cadres représentant des organes ou des fonctions n'étant représentés. On comprendra que les interconnexions logiques sont telles que représentées sur la figure 2 et que les commandes d'opérations et le traitement des données sont effectués par le microprocesseur programmé 72.

Au moment où la carte de crédit 100 est délivrée à l'utilisateur éventuel par la banque un numéro d'identification personnel à six chiffres est également affecté à l'utilisateur. Ce numéro d'identification personnel peut facultativement se trouver dans une certaine relation avec les informations enregistrées sur une bande de matière magnétique portée par la carte de crédit 100. Lorsque la carte 100 est insérée dans le terminal 46, la présence d'une carte est détectée et un mécanisme d'entraînement des cartes de crédit entraîne la carte dans le terminal 14 et la fait passer devant une tête de lecture où la carte est vérifiée pour déterminer si elle est dans l'orientation convenable et dans un état convenable. Si la carte est mal orientée, si elle contient des données illisibles ou si elle est d'un type qui ne peut pas être accepté par le terminal 46, elle est rendue à l'utilisateur. (Si la carte est expirée, elle peut être retenue sur une commande de l'ordinateur hôte). Si l'on admet que la carte de crédit est convenable, la carte 100 est alors entraînée devant un lecteur de carte 102 qui lit les informations portées par la bande magnétique et les met en mémoire dans la partie à accès sélectif de la mémoire de données 74 et la carte est alors conservée dans la région de conservation des cartes en attente. La carte de crédit 100 est compatible avec les normes établies par l'"American Bankers Association". Ceci signifie que la bande magnétique contient une séquence de mots de cinq bits représentant un bit de parité et quatre bits de données. Les mots de données fixes sont : un caractère de début de message (SOM) un caractère séparateur de zones et un caractère de fin de message (EOM). Les chiffres sont indiqués dans la représentation décimale codée binaire. Un format de bande magnétique type commence par un caractère de début de message suivi par un numéro de compte pouvant comporter jusqu'à 19 caractères, un caractère de séparation de zones, quatre caractères spéficiant le mois et l'année de la date d'expiration de la carte de crédit, une zone de données discrétionnaires, un caractère de fin de message (EOM) et un caractère de contrôle longitudinal par redondance. 40 caractères de 5 bits peuvent être enregistrés au maximum sur la bande magnétique. Pendant que les caractères sont lus, une clé de sélection désignée K1, qui est prévue en tant qu'option d'initialisation, détermine un point de départ pour sélectionner 8 caractères séquentiels de la bande magnétique. Par exemple, si K1 contient le nombre 5, les caractères 5 à 13 suivant le caractère de départ de message SOM sont sélectionnés à l'étape 104, sans leurs bits de parité pour former 32 bits. Ces 32 bits sont traités suivant un algorithme de chiffrement 106 pour engendrer 32 bits de données chiffrées.

La comparaison de tout ou partie d'un numéro d'identification personnel avec les informations de la carte de crédit correspondante peut être sélectivement prévue, au choix de la banque cliente, et cèci est indiqué

au moment de l'initialisation. Si l'option de comparaison n'est pas sélectionnée, la correspondance entre les numéros d'identification et les informations de la carte de crédit peut être choisie de manière aléatoire. Cependant, l'exécution d'une comparaison de correspondance est alors impossible si le terminal 14 fonctionne sous la commande d'un processeur hôte "hors groupe", c'est-à-dire non connecté à l'ordinateur 12. Si l'option de contrôle local est sélectionnée, deux clés indiquent la manière suivant laquelle le contrôle est effectué.

La première clé de contrôle K1 permet la sélection d'un groupe contigü quelconque de 8 caractères lus sur la carte de crédit. La clé K1 identifie la position à la suite du caractère de début de message (SOM) du premier des 8 jaractères. Les huit caractères ne sont pas nécessairement choisis de façon à être tous compris à l'intérieur du numéro de compte de la carte de crédit. Dans le présent exemple K1 = 5 de sorte que les caractères 5 à 13 sont sélectionnés.

La seconde clé de contrôle K2 détermine ceux des chiffres du numéro d'identification personnel qui doivent être contrôlés en indiquant la position du chiffre auquel le contrôle doit commencer. Ainsi K2 = 1 a pour résultat que les chiffres 1 à 6 sont contrôlés, K2 = 4 a pour effet que les chiffres 4 à 6 sont contrôlés et K2 = 6 a pour effet que seul le chiffre le moins significatif est contrôlé. Lorsque le nombre des chiffres contrôlés s'accroit, (c'est-à-dire lorsque K2 est plus petit), la protection contre la fraude effectuée en essayant de deviner les numéros d'identification est accrue pour le fonctionnement avec un processeur hôte hors groupe. Cependant, les chiffres contrôlés localement doivent avoir une correspondance prédéterminée avec les informations de la carte de crédit tandis que les chiffres non contrôlés peuvent avoir une correspondance aléatoire. L'accroissement du nombre de chiffres contrôlés localement diminue ainsi le nombre de chiffres disponibles pour la correspondance aléatoire et accroit les possibilités d'accès au fichier central d'un ordinateur en groupe, auquel le terminal est connecté dans le cas où l'algorithme de correspondance et la clé de chiffrement sont violés. Dans le cas du présent exemple, on a supposé que la banque cliente a exercé son option en choisissant la caractéristique de contrôle local avec K2 = 4.

L'algorithme de chiffrement particulier qui détermine la correspondance entre les numéros d'identification et les informations de la carte de crédit est sans importance critique pour la mise en oeuvre de la présente invention excepté que la relation entre les données d'entrée en clair et les données de sortie chiffrées doit être fonction d'une clé de chiffrement désignée ici première clé de chiffrement, ou clé A. Aux fins de cet exemple, on a supposé que l'agorithme de chiffrement est du type appelé "Lucifer" dans un article

de H. Feistel, "Cryptography and Computer Privacy" , Scientific American, Mai 1973, pages 15 à 23, ou décrit dans un article de C.H. Meyer, "Enciphering Data for Secure Transmission ", Computer Design, avril 1974, pages 129 à 134. Une clé de chiffrement, telle que la clé A pour l'algorithme 106 est un mot contenant 64 chiffres binaires. La clé de chiffrement peut être également considérée comme comportant 8 octets de 8 bits. La clé A est mise en mémoire dans la partie de mémoire auxiliaire du sous-système des fonctions assurées par l'opérateur 76 et occupe 8 des 128 mots de cette mémoire. Afin d'assurer une protection complète de cette clé, la clé est détruite chaque fois qu'une fonction d'entretien à partir du panneau d'interface du client est nécessaire. Cette destruction empêche qu'une personne faisant partie du personnel d'un service d'entretien du terminal puisse avoir accès au code. Suivant un premier procédé, un employé de banque occupant une position de confiance ayant accès à la clé A attend jusqu'à ce que l'employé d'entretien ait achevé l'entretien du terminal puis entre le code de 64 bits sous forme de 8 paires de chiffres hexadécimaux entrés séparément. Un affichage hexadécimal sur le panneau de l'opérateur indique les chiffres entrés pour permettre une correction si nécessaire, seuls les deux derniers chiffres entrés étant affichés à un moment donné. Cette limitation de l'affichage à deux chiffres protège la sécurité de la clé en obligeant une personne qui essayerait de copier la clé en observant l'affichage d'observer l'affichage pendant une période de temps importante du fait que l'observation de la totalité de la clé en un seul et même instant est rendu impossible.

Cependant, selon un autre mode de réalisation, la clé A n'est pas communiquée à l'employé de banque de confiance mais une clé A' ayant une relation prédéterminée avec la clé A. Dans un mode de réalisation, l'employé de confiance entre la clé A' dans le terminal de la même manière que s'il entrait la clé A. Cependant, le terminal traite la clé A' avec un algorithme de chiffrement 108 qui peut être similaire, voir identique, à l'alogorithme de chiffrement 106 pour produire la clé de chiffrement A. L'algorithme de chiffrement 108 utilise une seconde clé de chiffrement, désignée clé C, qui est une clé auxiliaire du terminal, dans le processus qui convertit la clé A' en clé A. Alternativement, une clé complètement séparée peut être chargée au moment de l'initialisation à cette fin.

Du fait de la relation prédéterminée qui existe entre les 32 bits de la carte de crédit qui sont chiffrés avec la clé A et le numéro d'identification personnel de 6 chiffres qui est atrribué à une personne au moment où une carte est délivrée la sécurité de la clé A est extrêmement importante. Si une catégorie de cartes de crédit doit être utilisable dans plusieurs succursales d'une banque cliente, au moins une personne de chaque succursale

doit avoir accès à la clé A de sorte qu'elle peut entrer cette clé sur le clavier d'un terminal 46 chaque fois que cela est nécessaire. Pour un banque importante comportant de nombreuses succursales, cette distribution peut devenir très importante. En outre, si une carte de crédit doit pouvoir être utilisée de façon interchangeable dans plusieurs banques, toutes les banques qui acceptent la carte doivent avoir la même clé de chiffrement A. Le nombre de personnes ayant accès à la clé A est ainsi à nouveau accru et peut devenir très important. L'utilisation d'un algorithme de chiffrement 108 assure la sécurité vis à vis de cette large distribution de la clé A. En utilisant une clé C différente à chaque point d'activité bancaire, seule une clé A' prédéterminée correspondant à une clé C donnée fonctionne de la façon appropriée pour produire la clé A, d'importance primordiale. Par exemple, chaque point d'activité bancaire peut être une succursale de banque séparée ayant trois ou quatre terminaux 14. Seule la clé A' prévue pour ce point d'activité ou succursale de banque produit de la façon appropriée la clé A. Si une personne ayant accès à la clé A' dans une succursale se rend dans une autre succursale dans laquelle une clé C différente est utilisée dans l'algorithme de chiffrement 108, une clé A' de la première succursale ne produit pas la clé A dans la seconde succursale. Il est ainsi possible de limiter la distribution de la clé A à un très petit groupe de personnes soigneusement sélectionnées.

L'algorithme de chiffrement 106 produit ainsi 32 bits de sortie ayant une relation prédéterminée avec les 32 bits d'entrée. Ces 32 bits de sortie sont divisés en 6 mots de 5 bits au moyen d'un processeur de conversion à l'aide d'une table 110, 30 seulement des 32 bits étant utilisés. Par exemple, les mots peuvent être formés à partir des 6 premiers groupes de cinq bits séquentiels chacun, les deux derniers bits n'étant pas utilisés. Chaque groupe de cinq bits est utilisé dans le processus de conversion à l'aide d'une table 110 comme mot d'adresse pour accéder à une table qui conserve en mémoire un chiffre décimal ayant une valeur comprise entre 1 à 9 à chaque emplacement d'adresse.La conversion au moyen de la table donne ainsi 6 chiffres, chacun ayant une valeur comprise entre 1 et 9. Ces chiffres correspondent directement au numéro d'identification personnel et le chiffe 0 est exclus afin d'éviter les numéros d'identification personnels qui commencent par des zéros dans les positions de gauche et risquent de créer des confusions ou des entrées de longueur variable.

S'il est déterminé que les informations contenues sur la carte d e crédit sont en ordre, un panneau d'accès des utilisateurs est ouvert pour donner à l'utilisateur accès au dispositif d'affichage optique pour les utilisateurs et au clavier des utilisateurs 112. L'utilisateur reçoit l'instruct tion d'entrer son numéro d'identification personnel au moyen de la partie

numérique du clavier. Si l'utilisateur n'a pas entré six chiffres à l'intérieur d'une période de temps prédéterminée, un numéro d'identification incorrect est supposé avoir été entré et un réessai est suggéré. A la suite de l'entrée de six chiffres exactement, une partie ou la totalité d'un numéro d'identification entré est comparée au nombre de six chiffres engendré au moyen de la table de conversion 110. La clé K 2 indique celles des six paires correspondantes de chiffres qui doivent être comparées.

Dans cet exemple, on a supposé que K2 = 4 de sorte que les trois chiffres les moins significatifs ayant les positions 4, 5 et 6 sont comparés au cours de l'étape de comparaison 114. Si la comparaison est invalide, un numéro d'identification erroné est indiqué et l'utilisateur est invité à recommencer l'entrée du numéro d'identification. Si le numéro d'identification n'est pas convenablement entré après un certain nombre d'essais, par exemple 3, la demande de transaction est terminée et un message est transmis à l'ordinateur. A la suite d'une commande de l'ordinateur la carte de crédit est, de préférence, transportée jusqu'à une boite de retenue pour empêcher toute nouvelle utilisation de la carte en vue d'essayer de faire concorder un numéro d'identification avec une carte de crédit éventuellement volée. Alternativement, la carte de crédit peut être rendue à l'utilisateur. Une fois qu'il a été déterminé que les chiffres comparés d'un numéro d'identification entré au moyen du clavier concordent avec les chiffres correspondants qui ont été calculés à partir des informations de la care de crédit, les six chiffres de numéro d'identification personnel sont convertis en u n code binaire de 32 bits, à l'étape 116. A l'étape 116, les 24 premiers bits sont obtenus directement, des six chiffres entrés. Les 8 derniers bits ou un octet sont obtenus en traitant chaque paire séquentielle de chiffres à quatre bits comme un unique octet et en prenant le résultat d'opérations OU exclusif successives sur les positions binaires correspondantes des trois octets résultants pour obtenir le contenu de données de la position binaire correspondante du quatrième octet. D'autres moyens pour obtenir les 8 derniers bits d'informations sont acceptables tant que le procédé permet d'obtenir des informations qui soient fonction de la totalité des bits du numéro d'identification entré.

Ces 32 bits sont alors traités avec un algorithme de chiffrement 118 utilisant la clé A pour produire un numéro d'identification personnel chiffré de 32 bits. L'algorithme de chiffrement 118 peut être, d'une manière générale, un algorithme de chiffrement appropriée quelconque, mais dans le cas du présent exemple, on a admis qu'il était identique à l'algorithme de chiffrement 106. L'utilisation du même algorithme pour les deux processus de chiffrement permet l'utilisation du même programme enregistré ou des mêmes circuits logiques pour les deux processus. La clé de chiffrement pour l'algorithme 118 peut

être également, d'une manière générale, une clé appropriée quelconque. Cependant, dans le cas du présent exemple, on a supposé que l'algorithme 118 utilise une clé A qui est identique à la clé A utilisée par l'algorithme 106. Cet usage multiple de la même clé de chiffrement ainsi que du même algorithme de chiffrement réduit également la complexité du fonctionnement du terminal 14 et les dimensions de la mémoire de données requise. Les 32 bits qui résultent de l'algorithme de chiffrement 118 représentent ainsi un numéro d'identification personnel après chiffrement.

Les 32 bits du numéro d'identification personnel chiffré sont alors convertis à l'étape 120 en 6 chiffres de quatre bits, deux chiffres de quatre bits étant alors abandonnés. A l'étape 122, les deux chiffres abandonnés sont remplacés par deux chiffres de 4 bits de données variables. Le remplacement d'une partie des informations tirées du numéro d'identification par des informations variables empêche que la zone chiffrée soit une constante. D'une manière générale, les données variables peuvent être des données quelconques qui n'ont aucun rapport prédéterminé avec le numéro d'identification personnel et qui varient avec chaque message de demande de transaction. Dans ce mode de réalisation, les données variables sont constituées par le compte d'un compteur (CNTR) d'espèces pour les transactions de délivrance d'espèces et par un numéro de transaction (N) pour les autres transactions.

Les 32 bits qui résultent de la combinaison des six chiffres de quatre bits et des 8 bits de données variables sont alors traités par un algorithme de chiffrement 124 qui utilise une troisième clé de chiffrement B. L'algorithme de chiffrement 124 peut, d'une manière générale, être un algorithme de chiffrement approprié quelconque mais, dans le cas du présent mode de réalisation on a admis que l'algorithme 124 était identique à l'algorithme 118, à l'algorithme 106 et à l'algorithme 108. La clé B est une clé de chiffrement de 64 bits qui est reçue de l'ordinateur 12 au cours de l'initialisation et ne peut pas être modifiée sauf à la suite de la communication d'une nouvelle clé par l'ordinateur. L'alhorithme de chiffrement 124 produit 32 bits de données chiffrées qui sont assemblés dans un message de demande de transaction immédiatement après l'en-tête commune de 4 octets comme précédemment décrit.

Après que l'étape de comparaison 114 a au moins partiellement validé la carte de crédit, l'utilisateur reçoit l'instruction d'indiquer la transaction qu'il demande au moyen du clavier 112. L'utilisateur reçoit tout d'abord l'instruction d'indiquer le type de transaction qui est demandé et toutes les lampes d'éclairage de la partie de demande de transaction du clavier sont allumées. Lorsqu'une touche particulière qui, dans le présent cas, est la touche de transfert de fonds est actionnée, la lampe de la touche actionnée reste allumée tandis que toutes les lampes d'éclairage des autres

touches de la partie du clavier sont éteintes. L'utilisateur reçoit ensuite l'instruction de choisir le compte d'où les fonds doivent être transférés et les lampes d'éclairage de toutes les touches de la partie de compte débité du clavier sont allumées. Comme l'utilisateur choisit la touche "compte d'épargne débité", la lampe d'éclairage de cette couche reste allumée tandis que les lampes d'éclairage de toutes les autres touches de la partie de compte débité du clavier sont éteintes. L'utilisateur reçoit alors l'instruction de choisir le compte auquel les fonds doivent être transférés et toutes les lampes d'éclairage de la partie du compte crédité du clavier sont éclairées. A la suite de la sélection de la touche de "compte courant", la touche actionnée reste éclairée et les lampes d'éclairage de toutes les autres touches de la partie de compte crédité du clavier sont éteintes. Les lampes d'éclairage qui restent allumées constituent une récapitulation visible de vérification de sorte que l'utilisateur peut avoir une confirmation ou un rappel de l'état des données de demande de transaction qu'il a entré. Il peut changer d'avis à tout moment en retournant à une zone précédemment entrée, en actionnant une nouvelle touche et en continuant le processus d'entrée des données au moyen du clavier à partir de ce point. Les informations numériques telles que le montant en espèces des fonds qui doivent être transférés sont entrées au moyen de la partie numérique du clavier 112. Toutes les informations numériques entrées sont affichées à titre de confirmation, sauf le numéro d'identification personnel. Ce numéro n'est pas affiché afin d'empêcher qu'une personne se tenant derrière l'utilisateur puisse obtenir subrépticement une connaissance du numéro d'identification personnel. Les données du clavier, les données de la carte de crédit lues sur la bande magnétique et toutes les données additionnelles désirées sont alors introduites en clair à la suite de la zone d'en-tête commune de quatre octets et de la zone chiffrée de quatre octets. Ces informations sont alors communiquées à l'ordinateur 12 en tant que message de demande de transaction.

2 - Message de réponse de transaction

Sur la figure 4 à laquelle on se réfèrera maintenant, on voit que lorsqu'un message de demande de transaction est reçu par l'ordinateur 12, il est soumis à un traitement, à l'étape 140, pour séparer les diverses zones de données, la zone d'en-tête commune étant utilisée pour acheminer le message, les 32 bits chiffrés étant traités par un algorithme de déchiffrement 142 et le texte en clair étant reçu par le processeur de données 144 qui comporte une mémoire de données de grande capacité 146. L'algorithme de déchiffrement 142 utilise la clé B qui est la même troisième clé, ou clé de transmission, qui a été utilisée par l'algorithme de chiffrement 124. Le processeur de données 12 utilise les données en clair pour accéder au dossier (fiche) de l'utilisateur

le fichier central contenu dans la mémoire de données 146. Cette fiche contient les données du compte ainsi que les informations correspondant à la carte de crédit de l'utilisateur telles que le numéro (ou les numéros) d'identification personnel.

Les 32 bits qui sont engendrés par l'algorithme de déchiffrement 142 sont transmis à un processeur de séparation 144 dans lequel les 6 chiffres de 4 bits du numéro d'identification personnel chiffré sont séparés des deux chiffres variables. Une comparaison est alors effectuée à l'étape 148, les 6 chiffres communiqués du numéro d'identification chiffre étant comparés aux 6 chiffres d'informations d'identification provenant de la fiche qui sont mis en mémoire sous forme chiffrée.

Ce processus de chiffrement améliore considérablement la sécurité des espèces mises en réserve dans les divers terminaux de transaction 14 qui peuvent être en communication avec un ordinateur hôte en groupe ou connecté. Une personne ayant une intention frauduleuse, qui a connaissance de la correspondance entre les numéros de compte de cartes de crédit et les numéros d'identification personnels pourrait subrépticement obtenir les espèces du terminal 14. Par exemple, une personne pourrait contrefaire ou voler des cartes de crédit comportant des informations qui correspondent à des comptes d'utilisateurs effectifs. En utilisant la carte de crédit contrefaite et le numéro d'identification personnel correspondant, une personne pourrait tout d'abord s'enquérir de la situation des divers comptes d'épargne, comptes courants et autres qui sont accessibles par l'intermédiaire de la carte de crédit. Ayant obtenu les informations de situation, cette personne pourrait alors utiliser la carte de crédit et le terminal de délivrance d'espèces 14 pour retirer des espèces de ces comptes jusqu'à ce que ces comptes ou la réserve d'espèces du terminal soient épuisés. Des comptes supplémentaires avec leur carte de crédit et le numéro d'identification personnel correspondant pourraient être utilisés d'une manière similaire jusqu'à ce que toutes les espèces disponibles au terminal de délivrance d'espèces aient été délivrées. La personne pourrait alors se rendre à d'autres terminaux pour épuiser les espèces de ces autres terminaux de délivrance d'espèces du système en utilisant de nouvelles cartes de crédit et numéros d'identification personnels. Du fait que chaque terminal de délivrance d'espèces 14 peut contenir plusieurs dizaines de milliers de francs et du fait qu'il y a de nombreux terminaux 14 en communication avec l'ordinateur 12, il devient extrêmement important de maintenir assurée la sécurité de la correspondance entre les numéros de compte des cartes de crédit et les numéros d'identification personnel et, cependant, de permettre des contrôles locaux afin d'accroître la disponibilité des terminaux 14 pour un fonctionnement hors groupe. Il devient extrêmement

difficile à une personne mal intentionnée d'obtenir la correspondance entre les informations de la carte de crédit et les numéros d'identification personnels lorsque les techniques décrites ici sont employées. Même si le numéro d'identification personnel peut être complètement engendré par traitement des informations de carte de crédit mises en mémoire au moyen de l'algorithme des chiffrements 106, la sécurité de sa clé de chiffrement A est maintenue comme décrit ci-dessus.

Si la relation entre une partie par exemple les trois premiers chiffres (ou de préférence la totalité) du numéro d'identification personnel et les informations de la carte de crédit mises en mémoire n'est pas en relation prédéterminée il devient encore plus difficile de compromettre la bonne marche du système. Il est possible que le personnel du centre de traitement des données où se trouve l'ordinateur 12 puisse avoir accès au numéro d'identification chiffré mis en mémoire. Cependant, le numéro d'identification personnel effectif n'est pas mis en mémoire dans l'ordinateur et le numéro d'identification chiffré est sans valeur pour obtenir des espèces d'un terminal 14 étant donné que c'est le numéro d'identification personnel qui doit être entré au moyen du clavier d'un terminal 14. Il est ainsi nécessaire pour une personne qui cherche à obtenir la correspondance entre un grand nombre de cartes de crédit et les numéros d'identification personnels correspondants d'avoir accès à la fois aux numéros d'identification personnels chiffrés mis en mémoire dans le fichier central de l'ordinateur et l'algorithme de déchiffrement correspondant à l'algorithme de chiffrement 118 et à la clé de chiffrement A.

Lorsque les cartes de crédit sont délivrées, il est possible de limiter la connaissance de la correspondance entre les données de la carte de crédit et les numéros d'identification personnels à un tout petit nombre de personnes. En fait, les comptes peuvent être établis de telle sorte qu'une partie du numéro d'identification personnel soit calculée à partir des informations de la carte de crédit et qu'une partie soit engendrée de façon aléatoire par un ordinateur. Le numéro d'identification personnel total peut alors être imprimé et mis dans une enveloppe cachetée avec une carte de crédit de telle sorte que le numéro d'identification personnel ne peut être observé visuellement que lorsque l'enveloppe est donnée à un utilisateur éventuel au moment où il ouvre un compte comportant une carte de crédit qui peut être traité par un terminal 14. Il est ainsi possible de réaliser un système d'affectation dans lequel aucun membre du personnel de la banque n'a accès à la correspondance entre les comptes à cartes de crédit et les numéros d'identification personnels correspondants.

Si la comparaison effectuée à l'étape 150 montre que les numéros

d'identification personnels chiffrés en mémoire et communiqués ne sont pas identiques, l'ordinateur assemble et communique un message de réponse de transaction indiquant que l'exécution de la transaction n'est pas autorisée. Le message de réponse de transaction donne au terminal demandeur 14 l'instruction de retenir la carte de crédit ou de la rendre à l'utilisateur. Par contre, s'il est déterminé que les numéros d'identification chiffrés en mémoire et communiqués correspondent et si la transaction demandée n'enfreint aucune des règles prédéterminées qui peuvent concerner les montants en francs, la fréquence de retraits ou les soldes des comptes, la transaction est autorisée par un message de réponse de transaction. Le message de réponse de transaction contient 32 bits d'informations chiffrées correspondant aux 32 bits d'informations chiffrées qui sont reçus dans le message de demande de transaction. Au cours d'un assemblage, à l'étape 152, 32 bits sont assemblés en vue d'être chiffrés au moyen de l'algorithme de chiffrement 154 en utilisant la clé B, qui est la troisième clé de chiffrement ou clé de transmission. L'algorithme de chiffrement peut, en général, être un algorithme de chiffrement approprié quelconque mais, dans le cas du présent exemple, on a admis que cet algorithme est identique aux algorithmes de chiffrement 106, 118 et 124. On a admis en outre que la clé B est identique à la clé B utilisée avec l'algorithme de chiffrement 124. Les 32 bits qui sont assemblés pour le chiffrement sont différents des 32 bits communiqués qui contenaient les 6 chiffres du numéro d'identification chiffré et deux chiffres variables. Les 32 bits du message de réponse de transaction comprennent un compte de compteur d'espèces d'un octet, correspondant à un premier compte d'espèces (CNTR1) calculé par un terminal 14 qui est incrémenté chaque fois qu'un billet est délivré, un octet d'action qui indique la réponse que le terminal 14 doit apporter à la transaction d'utilisateur demandée, un octet de second compteur d'espèces (CNTR2) identifiant le compte d'espèces qui est calculé pour un second mécanisme de délivrance d'espèces contenu dans le terminal 14 et un octet de montant (AMT) qui indique le nombre de billets qui convient pour la transaction demandée. Ces 32 bits sont alors traités au moyen de l'algorithme de chiffrement 154 pour former 32 bits chiffrés 156. Les bits chiffrés 156 sont alors combinés aux données en clair, telles que les données d'affichage facultatives, les données de reçu faculatatives ou des données additionnelles nécessaires pour compléter la transaction et l'ensemble est communiqué en retour au terminal demandeur 46 sous forme de message de réponse de transaction.

3 - Exécution et message d'état

Lorsque le message de réponse de transaction est reçu par le terminal 14, il est soumis à un traitement d'entrée, pour contrôler l'exactitude

de la transmission et séparer le message de réponse en ses diverses zones. La zone chiffrée est traitée par un algorithme de déchiffrement qui utilise la clé B pour rétablir les 32 bits contenant l'octet de compteur d'espèces N°1 (CNTR1), l'octet d'action, l'octet du compteur d'espèces N°2 (CNTR2) et l'octet des données de montant (AMT). Ces octets sont contrôlés pour vérifier leur exactitude afin d'assurer que le message de réponse de transaction a été transmis sans erreur et qu'il correspond au message de demande de transaction correct. Un règlement de transaction est alors exécuté, conformément au contenu du message de réponse de transaction. Lorsqu'il effectue le règlement de la transaction, le terminal 14 rend ou retient la carte de crédit, délivre les documents appropriés, tels que des espèces ou des états de transaction imprimés, exécute formellement ou annule la transaction, affiche les messages appropriés pour permettre à l'utilisateur de manifester son accord ou son refus et exécute toutes les autres fonctions de règlement de transaction qui sont nécessaires pour l'achèvement de la transaction.

A la suite de l'achèvement d'une transaction demandée par un utilisateur, le terminal 14 communique un message d'état à l'ordinateur 12 pour l'informer de la manière suivant laquelle la transaction demandée a été achevée et de l'état du terminal 14. La préparation du message d'état comporte l'assemblage, de 32 bits qui sont chiffrés à l'aide d'un algorithme utilisant la clé B pour engendrer 32 bits chiffrés. L'algorithme de chiffrement peut être, d'une manière générale, un algorithme de chiffrement approprié quelconque mais dans le cas du mode de réalisation préférentiel décrit ici, l'algorithme de chiffrement est identique aux algorithmes de chiffrement 106, 108, 118, 124 et 154. La clé B est identique à la clé utilisée pour les algorithmes 124 et 152. Cependant, à la différence de la clé A, la clé B peut être modifiée par l'ordinateur 12 et il est envisagé que la clé B soit changée de temps à autre. Les 32 bits sont soumis à un traitement de sortie en étant combinés aux informations d'état non chiffrées et sont transmis sous forme de message d'état du terminal d'exécution de transactions 14 à l'ordinateur hôte 12.

Le procédé consistant à utiliser des algorithmes de chiffrement, comme décrit ici, assure une grande sécurité pour le système d'exécution de transactions 10 sans nécessiter une capacité de mémoire élevée nécessaire pour stocker de multiples programmes de chiffrement. En outre, si l'on choisit convenablement les algorithmes de chiffrement et e déchiffrement, l'algorithme de déchiffrement peut être entièrement similaire à l'algorithme de chiffrement pour permettre un usage double de la plus grande partie du programme d'algorithme de chiffrement tant pour le chiffrement que pour le déchiffrement. Il en résulte des économies supplémentaires en ce qui concerne les besoins de mémoire de programmes. Le dernier chiffrement des 32 bits d'informations

chiffrées dans les trois messages de transaction d'utilisateur permet d'assurer la sécurité du numéro d'identification chiffré au cours de sa transmission par les canaux de communication tout en permettant que le même format général soit utilisé pour les trois messages. Dans le message de demande de transaction, le processus d'assemblage combine le numéro d'identification chiffré à des données variables afin de rendre extrêmement difficile à une personne qui surveillerait les lignes de communication de découvrir la clé B et l'algorithme de chiffremennt en entrant de manière répétitive le même numéro d'identification, la même carte de crédit et la même demande et en contrôlant les communications chiffrées correspondantes. Le message de réponse de transaction contient un octet de compteur N°1, un octet d'action, un octet de compteur N°2 et un octet de montant. Ces informations sont totalement différentes des informations codées du message de demande de transaction et contiennent également des informations variables. L'octet de montant et l'octet d'action auront tendance à être les mêmes pour les mêmes types de demande de transaction, cependant les octets des comptes seront différents. Les 32 bits chiffrés du message d'état sont différents des zones chiffrées des deux autres messages, étant donné qu'ils contiennent le numéro de transaction qui varie avec le temps, les octets des compteurs N°2 et N°1 dans des positions d'octets différents de celles qu'ils occupent dans le message de réponse de transaction et un octet de compte (CB) qui indique (au moyen d'un compte binaire) le nombre d'octets de données d'état et d'interrogation qui suivent la partie chiffrée du message dans le cas d'un message d'état normal. Un message d'état qui est engendré en réponse à une fin de transaction ne contient pas normalement d'octet de données d'interrogation. Dans le cas où le message d'état est un message d'état d'exception du type "rétablissement de demande", le troisième octet (CB) de la zone chiffrée contient l'octet "d'action" du message de réponse de transaction pour la dernière demande. Ainsi, en changeant de temps à autre la clé B et en transmettant des informations différentes dans la partie chiffrée de chaque type différent de message la tâche consistant à découvrir l'algorithme de chiffrement de transmission et à trouver la clé B utilisée en contrôlant les lignes de communication est rendue extrêmement difficile. Même si l'algorithme de chiffrement de transmission et la clé B étaient découverts, la surveillance de la transmission des messages ne permettrait d'établir une correspondance entre les comptes et les numéros d'identification personnels chiffrés que pour des cartes de crédit spécifiques utilisées pendant la surveillance des lignes de communication. La réunion d'un grand nombre de cartes de crédit volées ou contrefaites et des numéros d'identification personnels ne pourrait être réalisée qu'en découvrant en outre la clé A. Dans un mode de réalisation alternatif, dans lequel

il existe une relation prédéterminée entre tous les chiffres du numéro d'identification personnel et les informations de la carte de crédit, l'accès au fichier central n'est pas nécessaire. Les clés K1 et K2 assurent naturellement une sécurité supplémentaire au numéro d'identification chiffré dans le cas où l'option de contrôle local d'identification est utilisée.

Bien que l'on ait décrit dans ce qui précède et représenté sur les dessins les caractéristiques essentielles de l'invention appliquées à un mode de réalisation préféré de celle-ci, il est évident que l'homme de l'art peut y apporter toutes modifications de forme ou de détail qu'il juge utiles, sans pour autant sortir du cadre de ladite invention.

REVENDICATIONS

1.- Système de traitement de transactions du type comportant un ordinateur hôte et plusieurs terminaux de transaction qui sont connectés et dépendent dudit ordinateur hôte pour l'approbation et l'enregistrement de transactions indiquées par un utilisateur, chacun desdits terminaux étant caractérisé en ce qu'il comporte:

un dispositif d'entrée de données pour permettre l'entrée d'un bloc de données d'identification et d'une séquence de données propres à l'utilisateur;

un premier dispositif de codage connecté de façon à coder au moins une partie dudit bloc de données d'identification pour produire un premier ensemble chiffré de données d'identification indicatif d'au moins une partie dudit bloc de données d'identification;

un second dispositif de codage connecté de façon à coder au moins une partie dudit premier ensemble chiffré pour produire un second ensemble chiffré de données d'identification indicatif d'au moins une partie dudit bloc de données d'identification; et

un moyen de transmission connecté pour transmettre au moins une partie dudit second ensemble chiffré audit ordinateur hôte .

2.- Système selon la revendication 1 caractérisé en ce que chacun desdits terminaux comporte en outre un dispositif pour engendrer un bloc de données variables qui changent à chaque transaction d'utilisateur, et en ce que ledit second dispositif de codage est connecté de façon à coder ledit bloc de données variables avec au moins une partie dudit premier ensemble pour produire ledit second ensemble chiffré indicatif à la fois des données variables et d'au moins une partie dudit bloc de données d'identification.

3.- Système selon l'une des revendications 1 et 2 caractérisé en ce que chacun desdits terminaux comporte en outre des moyens pour mettre en mémoire une première et une seconde clés de chiffrement, et en ce que lesdits premier et second ensembles chiffrés sont produits respectivement en réponse auxdites première et seconde clés.

4.- Système selon la revendication 3 caractérisé en ce qu'il comporte en outre :

un panneau de commande d'opérateur pour entrer des informations déterminées par l'opérateur et,

un moyen pour mettre en mémoire une troisième clé de chiffrement,

ladite première clé de chiffrement étant produite en réponse à ladite troisième clé de chiffrement et aux informations entrées au moyen dudit panneau de commande.

5.- Système selon l'une quelconque des revendications 1 à 4 caractérisé en ce que ledit bloc de données d'identification a une longueur inférieure à une longueur prédéterminée,chacun desdits terminaux comportant en outre des moyens de génération connectés de façon à recevoir ledit bloc de données d'identification du dispositif d'entrée des données, pour engendrer un bloc résultant de données de longueur prédéterminée en ajoutant des caractères dépendant des données dudit bloc de données d'identification, et appliquer ledit bloc résultant audit premier dispositif de codage pour obtenir ledit premier bloc chiffré.

6.- Système selon l'une quelconque des revendications 1 à 5 caractérisé en ce que

ledit dispositif d'entrée de données de chacun desdits terminaux comporte en outre un moyen d'entrée de carte pour recevoir une carte d'identification de l'utilisateur comportant ladite séquence de données préalablement enregistrée sur la carte

chacun desdits terminaux comporte en outre un troisième dispositif de codage pour coder une partie prédéterminée de ladite séquence de façon à obtenir une séquence chiffrée, et un comparateur connecté de façon à comparer au moins une partie dudit bloc de données d'identification reçu par ledit dispositif d'entrée à au moins une partie de ladite séquence chiffrée de façon à indiquer l'identité ou la non identité des données comparées.

7.- Système selon la revendication 8 caractérisé en ce que chacun desdits terminaux comporte des moyens fonctionnant en réponse à l'indication de non identité de façon à empêcher la transmission de tout ou partie dudit second ensemble chiffré audit ordinateur.

8.- Système selon l'une quelconque des revendications précédentes caractérisé en ce que:

ledit ordinateur fonctionne de façon à gérer une pluralité de comptes, à approuver ou désapprouver des transactions demandées portant sur lesdits comptes et à modifier ces derniers en conformité avec les transactions demandées et approuvées qui portent sur ces comptes, chacun desdits comptes étant associé audit bloc de données d'identification et à ladite séquence de

données fournies par l'utilisation au dispositif d'entrée d'un terminal; ledit ordinateur n'approuvant pas une transaction demandée et modifiant le compte correspondant que lorsque des combinaisons de données indicatrices dudit bloc de données et de ladite séquence associées audit compte sont incluses dans une demande de transaction reçue par ledit ordinateur.

9.- Système selon la revendication 8 caractérisé en ce que chacun desdits terminaux comporte des moyens pour délivrer des espèces à un utilisateur en réponse à l'envoi par ledit ordinateur hôte d'un message d'approbation de délivrance d'espèces au terminal à la suite d'une demande de transaction de délivrance d'espèces par ledit terminal.

10.- Dans un système de traitement de transactions, entre un ordinateur conservant en mémoire des informations relatives à une pluralité de comptes d'utilisateurs, ces informations comportant un premier et un second blocs de données, et une pluralité de terminaux, procédé pour établir une transaction à la demande d'un utilisateur à l'un desdits terminaux caractérisé par les étapes suivantes:

le terminal qui reçoit la demande, transmet un premier message audit ordinateur contenant un premier et un second ensembles de données et des informations de demande de transaction,

ledit ordinateur accède aux informations en mémoire relatives au compte dont ledit premier bloc de données correspond audit premier ensemble de données, et compare ledit second ensemble de données audit second bloc de données,

ledit ordinateur communique un second message audit terminal, indiquant une désapprobation de la transaction demandée à moins que ledit second ensemble de données corresponde audit second bloc de données,

ledit terminal exécute la transaction demandée lorsque ledit second message indique que ledit ensemble de données correspond audit second bloc de données,

ledit terminal transmet un troisième message audit ordinateur, indiquant que la transaction demandée a été exécutée par ledit terminal,

ledit ordinateur met à jour les informations en mémoire pour le compte sur lequel a passé la transaction exécutée, en réponse à la réception dudit troisième message.

11.- Procédé selon la revendication 10 caractérisé en ce que ledit terminal auquel est demandé une transaction

reçoit ledit premier ensemble de données, un troisième ensemble de

données et des informations de demande de transaction d'un utilisateur de terminal,

traite ledit troisième ensemble de données conformément à un algorithme prédéterminé pour engendrer ledit second ensemble de données de façon à communiquer audit ordinateur ledit premier message contenant ledit premier ensemble de données, ledit second ensemble de données et les informations de demande de transaction reçues.

12.- Procédé selon la revendication 11 caractérisé en ce que ledit terminal

combine ledit second ensemble de données à des informations qui varient avec chaque transaction,

chiffre les données combinées pour engendrer un quatrième ensemble de données,

communique ledit quatrième ensemble de données en tant que partie dudit premier message audit ordinateur, ledit second ensemble de données n'étant contenu dans ledit premier message qu'en tant que partie dudit quatrième ensemble de données, ledit ordinateur déchiffrant ledit quatrième ensemble de données contenu dans ledit premier message pour obtenir ledit second ensemble de données.

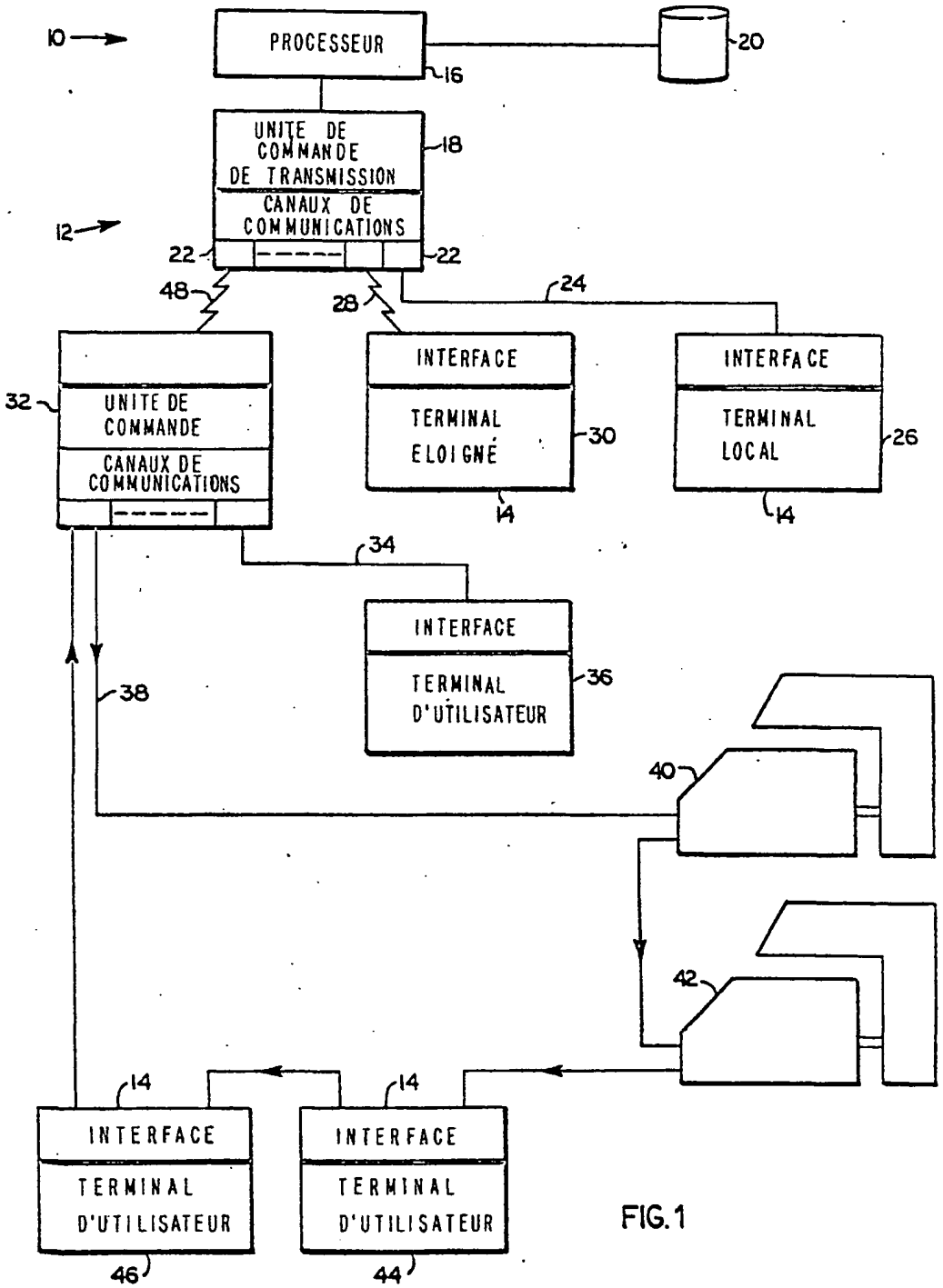
10
PROCESSEUR
16
20
UNITE DE COMMANDE DE TRANSMISSION
CANAUX DE COMMUNICATIONS
18
12
22
22
48
28
24
32
UNITE DE COMMANDE
CANAUX DE COMMUNICATIONS
INTERFACE
TERMINAL ELOIGNÉ
30
14
INTERFACE
TERMINAL LOCAL
26
14
34
INTERFACE
TERMINAL D'UTILISATEUR
36
38
40
42
14
14
INTERFACE
TERMINAL D'UTILISATEUR
INTERFACE
TERMINAL D'UTILISATEUR
46
44

FIG.1

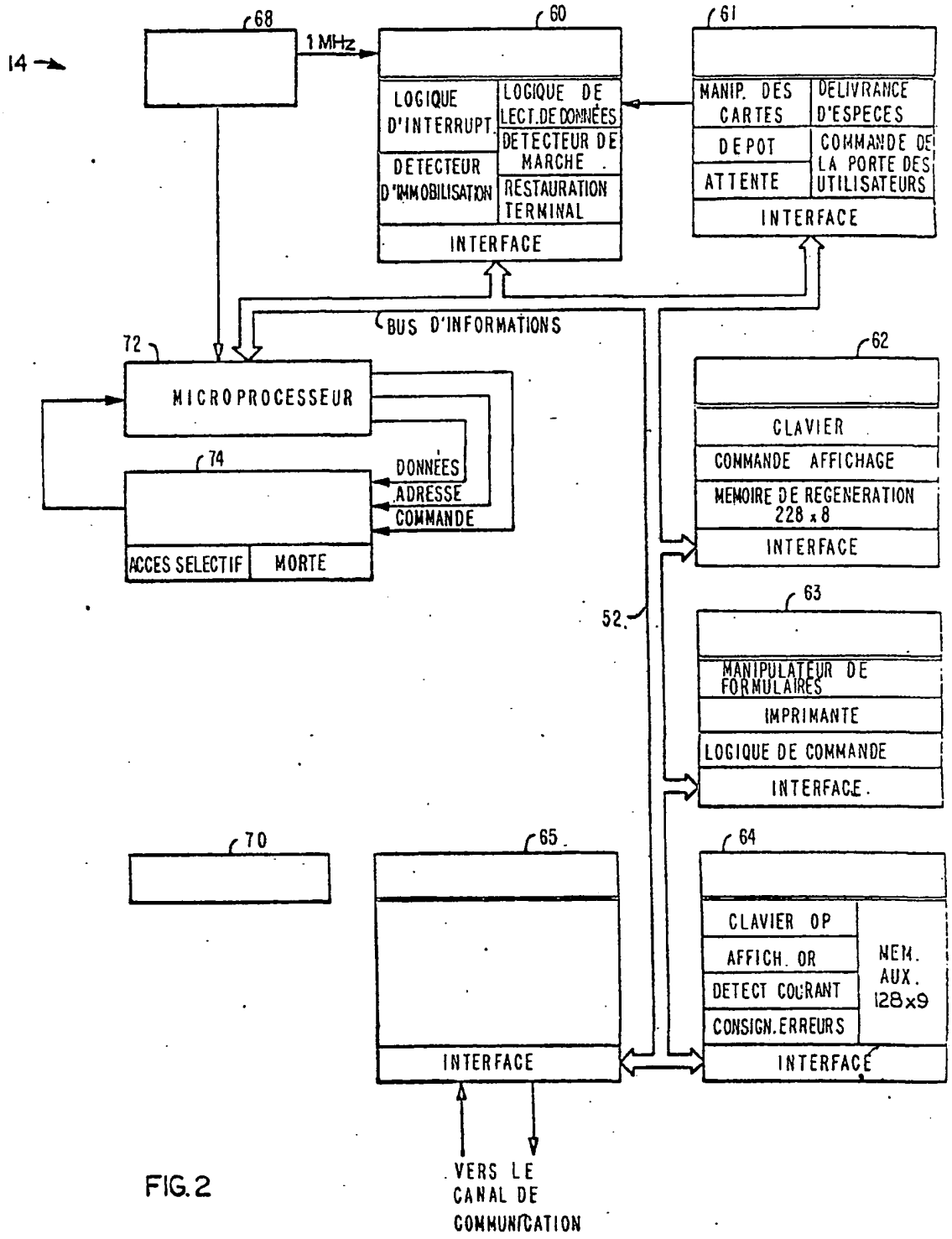
14
68
1 MHz
60
61
LOGIQUE D'INTERRUPT.
LOGIQUE DE LECT. DE DONNÉES
DETECTEUR DE MARCHE
DETECTEUR D'IMMOBILISATION
RESTAURATION TERMINAL
INTERFACE
MANIP. DES CARTES
DELIVRANCE D'ESPECES
DEPOT
COMMANDE DE LA PORTE DES UTILISATEURS
ATTENTE
INTERFACE
BUS D'INFORMATIONS
72
MICROPROCESSEUR
74
DONNÉES
ADRESSE
COMMANDE
ACCES SELECTIF
MORTE
62
CLAVIER
COMMANDE AFFICHAGE
MEMOIRE DE REGENERATION 228 x 8
INTERFACE
52
63
MANIPULATEUR DE FORMULAIRES
IMPRIMANTE
LOGIQUE DE COMMANDE
INTERFACE
70
65
INTERFACE
64
CLAVIER OP
AFFICH. OR
DETECT COURANT
CONSIGN. ERREURS
MEM. AUX. 128x9
INTERFACE
VERS LE CANAL DE COMMUNICATION

FIG. 2

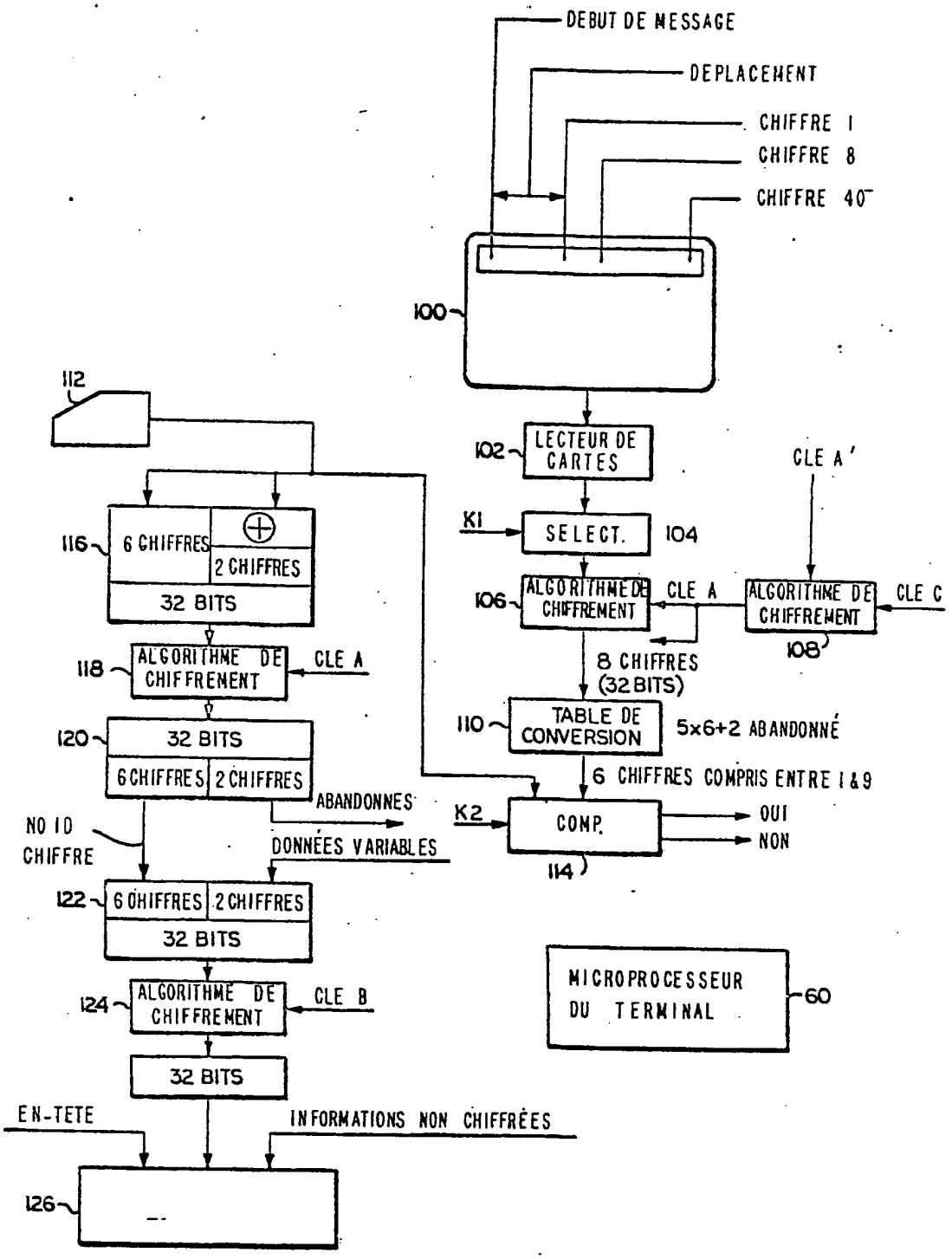
DEBUT DE MESSAGE
DEPLACEMENT
CHIFFRE 1
CHIFFRE 8
CHIFFRE 40
100
112
102
LECTEUR DE CARTES
CLE A'
K1
SELECT.
104
116
6 CHIFFRES
2 CHIFFRES
32 BITS
106
ALGORITHME DE CHIFFREMENT
CLE A
ALGORITHME DE CHIFFREMENT
CLE C
108
118
ALGORITHME DE CHIFFREMENT
CLE A
8 CHIFFRES (32 BITS)
110
TABLE DE CONVERSION
5x6+2 ABANDONNÉ
120
32 BITS
6 CHIFFRES
2 CHIFFRES
6 CHIFFRES COMPRIS ENTRE 1 & 9
ABANDONNES
K2
COMP.
OUI
NON
114
NO ID CHIFFRE
DONNÉES VARIABLES
122
6 CHIFFRES
2 CHIFFRES
32 BITS
MICROPROCESSEUR DU TERMINAL
60
124
ALGORITHME DE CHIFFREMENT
CLE B
32 BITS
EN-TETE
INFORMATIONS NON CHIFFRÉES
126

FIG. 3

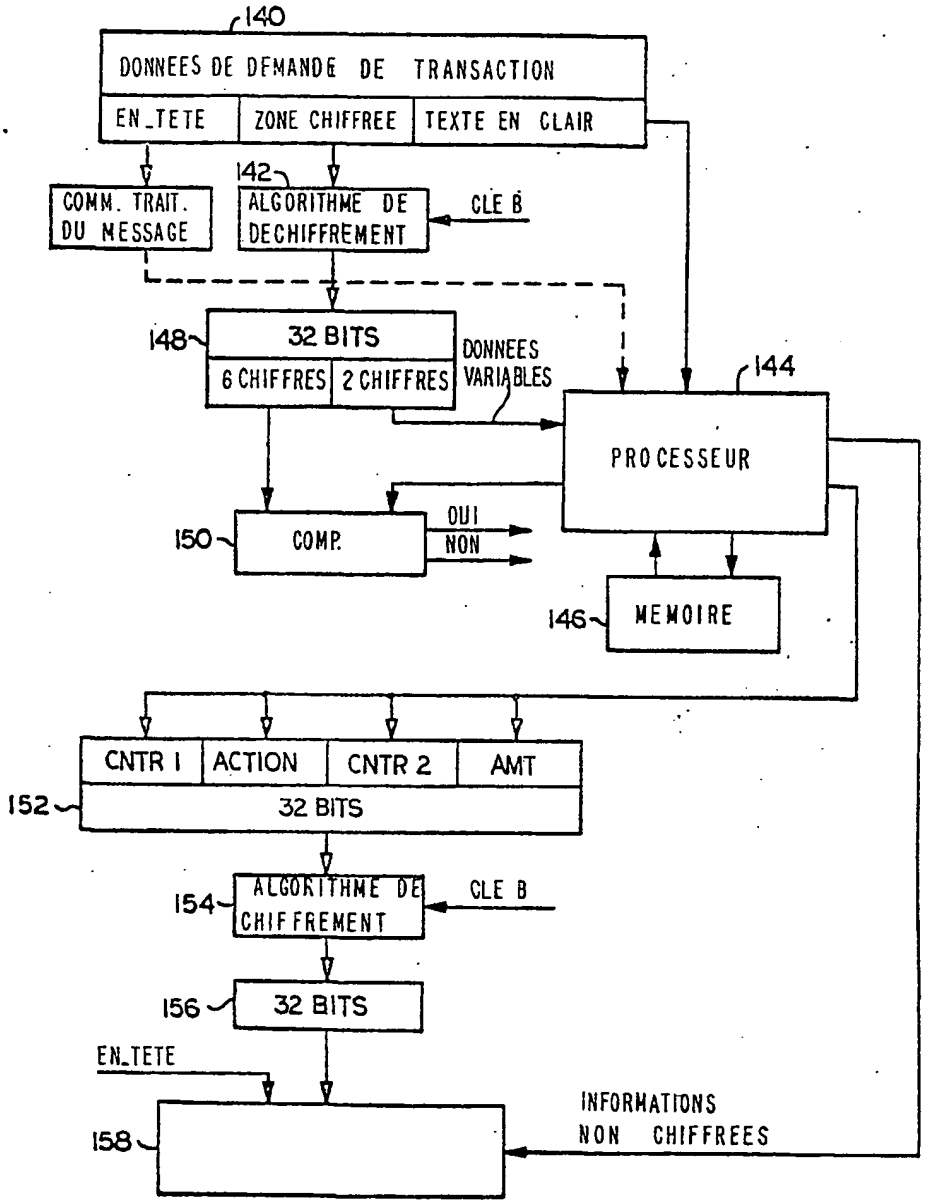
140
DONNEES DE DEMANDE DE TRANSACTION
EN_TETE
ZONE CHIFFREE
TEXTE EN CLAIR
142
COMM. TRAIT. DU MESSAGE
ALGORITHME DE DECHIFFREMENT
CLE B
148
32 BITS
6 CHIFFRES
2 CHIFFRES
DONNEES VARIABLES
144
PROCESSEUR
150
COMP.
OUI
NON
146
MEMOIRE
CNTR 1
ACTION
CNTR 2
AMT
152
32 BITS
154
ALGORITHME DE CHIFFREMENT
CLE B
156
32 BITS
EN_TETE
158
INFORMATIONS NON CHIFFREES

FIG. 4